(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2003 年12 月31 日 (31.12.2003)

PCT

(10) 国際公開番号
WO 2004/001701 A1

(51) 国際特許分類[7]: G09C 1/00, H03M 13/15, H04L 9/30, G06F 11/10

(21) 国際出願番号: PCT/JP2002/006166

(22) 国際出願日: 2002 年6 月20 日 (20.06.2002)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(71) 出願人 (米国を除く全ての指定国について): 株式会社 日立製作所 (HITACHI, LTD.) [JP/JP]; 〒101-8010 東京都 千代田区 神田駿河台四丁目６番地 Tokyo (JP).

(72) 発明者; および
(75) 発明者/出願人 (米国についてのみ): 外村 元伸 (TONOMURA,Motonobu) [JP/JP]; 〒185-8601 東京都 国分寺市 東恋ヶ窪一丁目２８０番地 株式会社 日立製作所 中央研究所内 Tokyo (JP). 近藤 雄樹 (KONDOH,Yuki) [JP/JP]; 〒185-8601 東京都 国分寺市 東恋ヶ窪一丁目２８０番地 株式会社 日立製作所 中央研究所内 Tokyo (JP).

(74) 代理人: 小川 勝男 (OGAWA,Katsuo); 〒103-0025 東京都 中央区 日本橋茅場町二丁目９番８号 友泉茅場町ビル 日東国際特許事務所 Tokyo (JP).

(81) 指定国 (国内): CN, JP, KR, US.

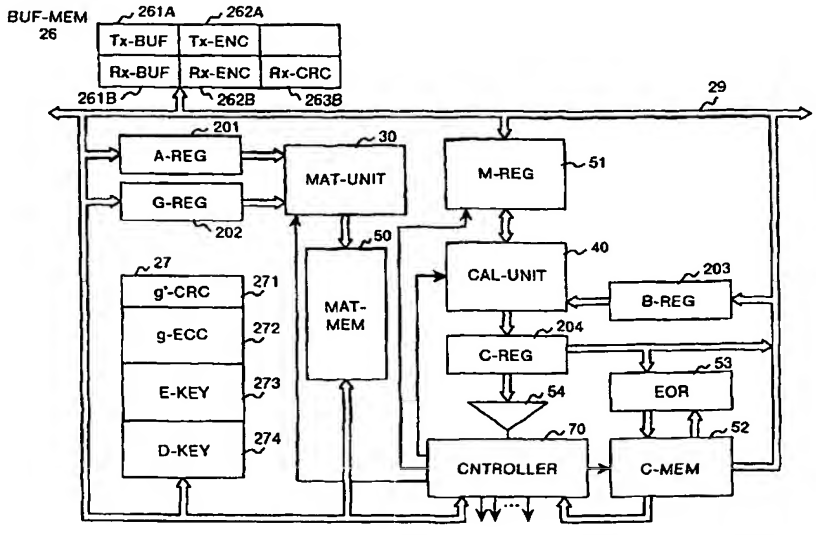
(84) 指定国 (広域): ヨーロッパ特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

(54) Title: CODE CALCULATING DEVICE

(54) 発明の名称: 符号演算装置



(57) Abstract: A product-sum calculating unit varies the parameters preset in first and second registers (201, 202) so as to instruct a matrix value calculating section (30) to calculate a matrix value for an error-detecting code (CRC) or for an elliptic curve cryptography (ECC). Then the unit changed the matrix value held in a matrix value register (51) so as to perform a product-sum calculation of the matrix value and data preset in a third register. Thus the unit is used commonly both for CRC encoding calculation and ECC encrypting calculation.

[続葉有]

WO 2004/001701 A1

(57) 要約:

第１、第２レジスタ２０１、２０２に設定されたパラメータを変えることによって、誤り検出符号（ＣＲＣ）用行列値又は楕円曲線暗号（ＥＣＣ）用行列値を行列値演算部３０で生成し、行列値レジスタ５１に保持する行列値を切替えることによって、前記行列値と第３レジスタに設定されたデータとの積和演算を実行する積和演算部をＣＲＣ符号化演算とＥＣＣ暗号化演算とに共用する。

明　細　書

符号演算装置

技術分野

本発明は、通信データ用の符号演算装置に関し、更に詳しくは、ディジタル・パケットデータの送受信において必要となる誤り検出(訂正)符号の生成とデータ暗号化／復号化処理のための符号演算装置に関する。

背景技術

ディジタル通信装置では、データの機密性保持およびネットワーク上での信号誤りの発生に備えて、パケットデータの暗号化／復号化機能と誤り検出(訂正)符号の生成機能が必要となる。音声データやテキストデータの他に、情報量の多い静止画像や動画像等の通信ニーズが増えるに従って、ディジタル通信装置には、データ転送速度の高速化に適した暗号化／復号化技術と誤り検出(訂正)符号の生成技術が要求されてきている。

データパケットの誤り検出符号としては、例えば、誤り訂正は行わずに誤り検出のみを目的としたＣＲＣ（Cyclic Redundancy Check Codes: 巡回冗長検査符号）がよく使われる。ＣＲＣ演算式については、例えば、Ramabadran, T.V. and Gaitonde S.S. “A Tutorial on CRC Computations”, IEEE Micro, vol.8、 No.4、pp.62-75、Aug.1988に記載されている。

一方、データの機密性を保持するために使用される暗号方式としては、ＲＳＡ暗号が有名である。しかしながら、ＲＳＡでは、暗号／復号鍵として１０２４ビットの長い符号を必要としているため、最近では、符号長が１６０ビット程度と短くて済む楕円曲線暗号（ECC:Elliptic Curve Cryptography）が注目されている。楕円曲線暗号処理に関する文献としては、例えば、Moon, S.、Park, J. and Lee, Y.、“Fast VLSI Arithmetic Algorithms

for High-Security Elliptic Curve Cryptographic Applications" IEEE Trans. Consumer Electronics、 vol.47、 No.3、pp.700-708、Aug.2001がある。上記文献には、楕円曲線暗号（ＥＣＣ）に必要な演算式と、ＥＣＣ処理を実現した大規模集積回路の１例について説明されている。

ＲＳＡは、桁上げ伝播が発生するモジュラー演算を採用しているため、ハードウェア量が多くなる。これに対して、ＥＣＣは、以下に説明するように、桁上げ伝播が発生しないガロア体（有限体）をベースにしているため、データの暗号／復号化をコンパクトなハードウェアで実現できる。

式（１）が示すガロア体上のｎ次多項式ｇ(x)によるモジュラー演算（mod）を考える。

$$g(x) = x^n + g_{n-1}x^{n-1} + \cdots + g_1x + 1 \qquad (1)$$

この多項式のガロア体は、一般にＧＦ（２ⁿ）と表記される。係数g_iの値は“０”または“１”であり、$g_i \in$ ＧＦ（２）と表記される。また、ＧＦ(2)の係数項内では、排他的論理和（ＥＯＲ）演算(⊕)が行われるが、本明細書では、特に混乱しない限り（+）演算子で代用する。

今、長さｎのデータを表現する次の３つの多項式について考える。

$$a(x) = \sum_{i=0}^{n-1} a_i x^i, \qquad b(x) = \sum_{i=0}^{n-1} b_i x^i, \qquad c(x) = \sum_{i=0}^{n-1} c_i x^i,$$

但し、a_i, b_i, $c_i \in$ ＧＦ（２）

ＥＣＣの場合、共通鍵または秘密鍵と呼ばれる暗号鍵を示すデータを多項式ａ(x)とし、この暗号鍵が適用される送受信データを多項式ｂ(x)とすると、送信側における暗号化データ、または受信側における復号化データ（元の平文データ）は、次式（２）の演算結果ｃ(x)として得られる。

$$c(x) \equiv a(x) \cdot b(x) \bmod g(x) \qquad (2)$$

式（２）を詳しく書くと、次式（３）にようになる。

$$\sum_{i=0}^{n-1} c_i x^i \equiv \left(\sum_{i=0}^{n-1} a_i x^i\right)\left(\sum_{i=0}^{n-1} b_i x^i\right) \bmod g(x) \qquad (3)$$

文献：Mastrovito, E.D., "VLSI Designs for Multiplication over Finite Fields GF(2ⁿ)"、Proc. Sixth Int'l Conf. 「Applied Algebra, Algebraic Algorithms, and Error-Correcting Codes (AAECC-6)」pp. 297-309, Jul. 1988と、公開公報WO 91/20028号（発明の名称「Universal Galois Field Multiplier」）において、Mastrovitoは、式（3）を次の行列形式に変換することを試みている。

$$\begin{bmatrix} c_0 \\ c_1 \\ \vdots \\ c_{n-1} \end{bmatrix} = \begin{bmatrix} m_{00} & m_{01} & \cdots & m_{0,n-1} \\ m_{10} & m_{11} & \cdots & m_{1,n-1} \\ \vdots & \vdots & \ddots & \vdots \\ m_{n-1,0} & m_{n-1,1} & \cdots & m_{n-1,n-1} \end{bmatrix} \begin{bmatrix} b_0 \\ b_1 \\ \vdots \\ b_{n-1} \end{bmatrix} \qquad (4)$$

$$c = M \cdot b \qquad (5)$$

式（4）におけるn×nの行列Mは、Mastrovito行列と呼ばれており、行列Mの値は、多項式a(x)とg(x)から前もって計算することができる。

一方、ＣＲＣの値は、送信メッセージ（または受信メッセージ）のデータを多項式b(x)で示した場合に、次式（6）で示すように、$x^n \cdot b(x)$を多項式g(x)で割った時に得られる余りc(x)として算出される。

$$c(x) \equiv x^n \cdot b(x) \bmod g(x) \qquad (6)$$

ここで、$x^n \cdot b(x)$は、データb(x)をnビット左シフトすることを意味しており、データの送信側では、式（６）で算出されたＣＲＣの値：多項式c(x)を送信データb(x)に加算した形で、伝送路に送出する。

データの受信側では、ＣＲＣ付きの受信データb(x)に対して同様の演算を行い、演算結果c(x)が０となった場合、極めて高い確率で受信

データ b(x)には誤りがないものと判定する。

式（２）と式（６）とを比較すると、ＣＲＣとＥＣＣの演算式が極めて類似していることがわかる。両者の違いは、ＣＲＣの場合、データ b(x)に乗算される値がｎ次の x^n であるのに対して、ＥＣＣの場合は、n-1 次の多項式 a(x)となっている点にある。

Mastrovito行列について述べた上記文献では、BCH や Reed-Solomon と呼ばれる誤り訂正方式を式（２）で一般的に取り扱おうとしているように思われる。しかしながら、上記文献には、これらの符号化方式を具体的にどのようにして式（２）に結びつけるかについて具体的な記載がない。また、後述する本発明が着目したＣＲＣ符号の行列表現に関して、上記文献には何ら示唆されていない。

発明の開示

本発明の目的は、誤り検出処理と暗号／復号化処理に共用できる符号演算装置を提供することにある。

本発明の他の目的は、誤り検出処理と暗号／復号化処理に共用できるガロア体(有限体)符号演算装置を提供することにある。

本発明の更に他の目的は、誤り検出処理用と暗号／復号化処理用の行列値を同一の行列値演算部で算出し、これらの行列値を選択的に利用して、誤り検出処理と暗号／復号化処理を行うようにした符号演算装置を提供することにある。

本発明の更に他の目的は、コンパクトなハードウェア構成で誤り検出処理と暗号／復号化処理を実行できるパケット通信装置を提供することにある。

これらの目的を達成するために、本発明では、ガロア体ベースのＣＲＣとＥＣＣの演算式の類似性に着目し、ＣＲＣ演算とＥＣＣ演算のためのハードウェアを共通化することを特徴とする。

ＣＲＣと楕円曲線暗号ＥＣＣの演算処理を共通化しようとした場合、容易に考えられる解決方法の１つは、式（２）で示したＥＣＣ演算でデータb(x)に乗算される多項式a(x)の次数をn－1次からn次に上げることによって、式（６）で示したＣＲＣ演算におけるx^nの次数と一致させておき、ＣＲＣ演算を行う場合は、多項式a(x)のn次の係数部を使用する方法である。しかしながら、このように多項式a(x)の次数を増やす方法では、本質的な解決策とはならない。

本発明では、ガロア体モジュロ演算がもつ次の性質を利用して、ＣＲＣとＥＣＣの演算処理を共通化する。

すなわち、式（１）が示すように、ガロア体モジュロ演算に適用される既約多項式g(x)は、x^nの係数g_nが“１”となっている。そこで、式（６）が示すＣＲＣ演算に適用されるn次以上の高次項x^nをg(x)でモジュロ演算し、n－1次以下の余りの項にリダクションすると、次の多項式（７）が得られる。

$$x^n \bmod g(x) \equiv g_{n-1}x^{n-1} + \cdots + g_1x + 1 \qquad (7)$$

ここで、式（７）の右辺を

$$g'(x) = g_{n-1}x^{n-1} + \cdots + g_1x + 1 \qquad (8)$$

と置き換えると、式（６）に示したＣＲＣの演算式は、次式（９）のように変形され、ＥＣＣの演算式（２）と同様に、データb(x)に乗算される多項式の次数をn-1次にすることができる。

$$c(x) \equiv g'(x)\cdot b(x) \bmod g(x) \qquad (9)$$

ＣＲＣの値は、a(x)に代えてg'(x)の値をセットすることにより、式（９）に従って算出できる。

また、x^nよりも更に高次の項x^{n+1}をg(x)でモジュロ演算すると、式（７）を利用して、次式（１０）が示すように、n-1次以下の項にリダクションできることが判る。

$$x^{n+1} \bmod g(x) \equiv g_{n-1}x^n + g_{n-2}x^{n-1} + \cdots + g_1x^2 + x$$
$$= g_{n-1}(g_{n-1}x^{n-1} + \cdots + g_1x + 1) + g_{n-2}x^{n-1} + \cdots + g_1x^2 + x$$
$$= (g_{n-1}g_{n-1}+g_{n-2})x^{n-1}+(g_{n-1}g_{n-2}+g_{n-3})x^{n-2}+\cdots$$
$$+(g_{n-1}g_2+g_1)x^2+(g_{n-1}g_1+1)x+g_{n-1} \qquad (10)$$

従って、n次以上の高次項は、n-1次以下の項にリダクションした後、x^iの係数項間を比較することによって、式（4）または（5）の行列値を得ることができる。

本発明の特徴の1つは、CRCの演算式を式（9）のように変形し、次数をECC演算式（3）に適合させることによって、同一の行列値演算部を利用して、ECC用行列値とCRC用行列値を計算できるようにしたことにある。また、本発明の他の特徴は、予め計算されたECC用行列値とCRC用行列値を選択的に利用することによって、同一の積和演算部で、ECC符号化／復号化演算とCRC演算を実行できるようにしたことにある。

図面の簡単な説明

第1図は、本発明が適用される誤り検出機能と暗号処理機能を備えたパケット通信装置の構成を示すブロック図。

第2図は、CRC誤り検出の符号化、復号化処理を説明するための図。

第3図は、ECC暗号化、復号化処理を説明するための図。

第4図は、行列演算回路30を備えた本発明による演算装置の1実施例を示すブロック図。

第5図は、行列演算回路30で生成される行列Mの計算値配列を説明するための図。

第6図は、n×nの行列Mの計算値を複数の部分行列に分割して生

成する場合の説明図。

第７図は、ＥＣＣ用の行列Ｍを構成する部分行列と入出力データとの関係を説明するための図。

第８図は、ＣＲＣとＥＣＣに共用される行列値演算部３０の１実施例を示す図。

第９図は、第４図に示したコントローラ７０が実行するＣＲＣ行列値生成ルーチン１００の１実施例を示すフローチャート。

第１０図は、コントローラ７０が実行するＥＣＣ用行列値生成ルーチン１２０の１実施例を示すフローチャート。

第１１図は、コントローラ７０が実行する送信データ処理ルーチン２００と受信データ処理ルーチン３００を示すフローチャート。

第１２図は、送信データ処理ルーチン２００における送信データ暗号化２１０の詳細を示すフローチャート。

第１３図は、送信データ処理ルーチン２００におけるＣＲＣ生成２３０の詳細を示すフローチャート。

発明を実施するための最良の形態

第１図は、本発明が適用されるデータ誤り検出機能と暗号処理機能を備えたパケット通信装置のブロック図を示す。

パケット通信装置は、コアプロセッサ(P-CORE)１０と、送受信データ処理部２０と、伝送路１３に接続された送信部１１および受信部１２とからなる。送信部１１と受信部１２は、伝送路１３が無線の場合、Ａ／Ｄ、Ｄ／Ａ変換器と、ＲＦ(Radio Frequency)処理部とを含み、伝送路１３がアナログ有線回線の場合は、モデム処理部を含む。

送受信データ処理部２０は、制御プロセッサ(P-CONT)２１と、暗号符号化部(ECC-ENC)２２、誤り検出符号化部(CRC-ENC)２３、誤り検出復号化部

(CRC-DEC)２４、暗号復号化部(ECC-DEC)２５と、バッファメモリ(BUF-MEM)２６、メモリ(MEM)２７からなり、これらの要素は、内部バス２９（２９A、２９B）によって相互接続されている。

コアプロセッサ１０から出力された送信メッセージ（平文データ）は、バッファメモリ２６の送信バッファ領域に一時的に格納され、送信データに機密保持が必要な場合は、送信メッセージが暗号符号化部２２で暗号化される。送信メッセージ（平文データまたは暗号化データ）は、誤り検出符号化部２３で生成した誤り検出符号を付加した形で、送信部１１から伝送路１３に送出される。

逆に、伝送路１３から受信した誤り検出符号付きの受信メッセージ（平文データまたは暗号化データ）は、受信部１２からバッファメモリ２６の受信バッファ領域に一旦格納され、誤り検出復号化部２４で受信メッセージの誤り検出符号の余り演算が行われる。余りがゼロの場合、受信データに誤りがないものと判断し、受信メッセージから誤り検出符号が除去される。誤り検出符号を取り除いた受信メッセージのデータが暗号文の場合、暗号復号化部２５で平文に戻した後、バッファメモリ２６を介してコアプロセッサ１０に転送される。誤り検出およびデータの暗号／復号化に必要な情報は、メモリ２７から読み出され、暗号符号化部２２、誤り検出符号化部２３、誤り検出復号化部２４、暗号復号化部２５は、制御プロセッサ２１に制御される。

第２図は、誤り検出にＣＲＣを適用した場合の誤り検出符号化部２３と誤り検出復号化部２４の動作を示す。

この場合、誤り検出符号化部２３では、送信データをｎビット長（ｎ＝３２ビット）のデータブロックｂ(x)に分割し、データブロック毎に符号化する。先ず、式（６）が示すように、データｂ(x)をｎビット左へシフト（$x^n \cdot b(x)$の演算）した後、これを予め指定された数値ｇ(x)で割って（モジュロ演算）、余りｒ(x)を求める。

$$r(x) \equiv x^n \cdot b(x) \mod g(x) \qquad (11)$$

次に、r(x)をデータ x^n b(x)に加算、すなわち、$w(x)=x^n \cdot b(x) \oplus r(x)$ の演算を行う。その結果、元のｎビットデータブロックは、２ｎビット長のデータブロック w(x)に変換した形で伝送路に送出される。

一方、受信側の誤り検出復号化部２４では、伝送路から受信したデータブロック $w'(x)= x^n \cdot b'(x) \oplus r'(x)$ に対して、送信側と同一の数値 g(x)でモジュロ演算を実行して、余りを求める。伝送路上で誤りが発生していなければ、次式（１２）が成立し、余り c(x)がゼロになる。

$$c(x) \equiv [x^n \cdot b'(x) \oplus r'(x) \mod g(x)]$$
$$= r'(x) \oplus r'(x) \qquad (12)$$

この場合、受信データ w'(x)から r'(x)を除去し、ｎビット右シフトすることによって、元のデータブロック b(x) = b'(x)を復元できる。尚、伝送路からの受信メッセージ長が２ｎビットよりも長い場合は、２ｎビット長のデータブロック毎に、上述した誤り検出復号化処理が繰り返される。

第３図は、暗号化にＥＣＣを適用した場合の暗号符号化部２２と暗号復号化部２５の動作を示す。

暗号符号化部２２では、送信データをｎビットのデータブロックに分割し、送信データブロックを多項式b(x)、共通鍵を多項式a(x)とし、既約多項式 g(x)でモジュロ演算を実行することにより、式(２)が示す暗号化データ c(x)を生成する。

ＥＣＣ暗号符号化データのブロック長ｎは、ＣＲＣよりも長い160ビット程度になるため、ＣＲＣと同一ハードウェアを適用するために、送信データブロック b(x)、共通鍵 a(x)、既約多項式 g(x)をそれぞれＣＲＣビット長に合わせた複数のサブブロック分割して、暗号化処理を繰り返す。

誤り検出符号が付加された暗号化データは、受信側で誤り検出され、もし、誤りがなければ、誤り検出符号を除去した暗号化データ c(x)に戻される。受信側の暗号復号化部２５では、次式（１３）が示すように、式(２)の a(x)、b(x)の代わりに秘密鍵 d(x)と受信データ c(x)を適用し、既約多項式 g(x)によってモジュロ演算を実行することによって、復号化されたデータ b(x)を得る。

$$b(x) \equiv d(x) \cdot c(x) \mod g(x) \qquad (13)$$

本発明の特徴は、上述した誤り検出符号化部２３、誤り検出復号化部２４、暗号符号化部２２、暗号復号化部２５に必要なハードウェアを共用することによって、送受信データ処理部２０の構成を簡単化したことにある。

第４図は、本発明による送受信データ処理部２０の１実施例を示す。

送受信データ処理部（符号演算装置）２０は、行列値演算部(MAT-UNIT)３０、積和演算部(CAL-UNIT)４０、制御部(CONTROLLER)７０と、バッファメモリ(BUF-NEM)２６、パラメータ格納用のメモリ２７、行列値格納用のメモリ(MAT-MEM)５０、行列値レジスタ(M-REG)５１、演算結果保持メモリ(C-MEM)５２と、パラメータレジスタ(A-REG、G-REG)２０１、２０２、データレジスタ(B-REG)２０３、符号レジスタ(C-REG)２０４と、EOR 加算回路５３と、一致検出回路５４からなる。

メモリ２７は、ＣＲＣ演算で必要となるリダクションされた多項式 g'(x)の記憶領域(g'-CRC)２７１と、ＥＣＣ演算で必要となる既約多項式 g(x)の記憶領域(g-ECC)２７２、暗号鍵（公開鍵）の記憶領域(E-KEY)２７３と、復号鍵（秘密鍵）の記憶領域(D-KEY)２７４とを含む。

また、バッファメモリ２６には、コアプロセッサ１０から供給された送信メッセージの格納領域(Tx-BUF)２６１Ａ、暗号化送信メッセージの格納領域(Tx-ENC)２６２Ａと、受信部から供給されたＣＲＣ付の受信メッセージの格納領域(Rx-CRC)２６３Ｂ、ＣＲＣ除去後の暗号化

受信メッセージの格納領域(Rx-ENC)２６２Ｂ、復号化された受信メッセージの格納領域(Rx-BUF)２６１Ｂとが定義され、コアプロセッサ１０と送受信データ処理部２０との間では、Tx-BUF領域２６１ＡとRx-BUF領域２６１Ｂを介してメッセージが送受信される。

本実施例で示した送受信データ処理部（符号演算装置）２０の動作モードには、行列値演算モードと、送信データ暗号化モードと、送信データ誤り符号化モードと、受信データ誤り検出モードと、暗号データ復号化モードとがある。これらの動作モードの切替えは、制御部７０が行う。

行列値演算モードにおいて、例えば、ＥＣＣ暗号化用の行列値を生成する場合は、制御部７０が、メモリ領域２７２から読み出した既約多項式g(x)の値をG-REG ２０２に設定し、メモリ領域２７３から読み出した暗号鍵をA-REG ２０１に設定した状態で、行列値演算部３０を起動する。生成された行列値は、メモリ５０の暗号化用行列領域に保持される。

同様に、ＥＣＣ復号化用の行列値は、メモリ領域２７２からG-REG ２０２に既約多項式g(x)の値を設定し、メモリ領域２７４からA-REG ２０１に復号鍵を設定した状態で生成され、行列値演算部３０で生成された行列値は、メモリ５０の復号用行列領域に保持される。

ＣＲＣ用の行列値は、A-REG ２０１とG-REG ２０２にメモリ領域２７１からg'(x)の値を設定した状態で生成され、行列値演算部３０で生成された行列値は、メモリ５０のＣＲＣ用行列領域に保持される。

ここで、A-REG ２０１とG-REG ２０２を、例えば、ＣＲＣ演算用のパラメータ長に合わせて３２ビット長とした場合、ＣＲＣ用の行列値は、これらのレジスタへの１回のパラメータロードで計算できる。しかしながら、ＥＣＣ演算のパラメータは、ＣＲＣ演算用のパラメータよりも長いため、ＥＣＣ暗号化用および復号化用の行列値は、後述するように、メモリ２７から既約多項式g(x)と暗号化鍵をそれぞれ３２ビット単位で分割して読み出し、レジス

タ２０１、２０２の設定パラメータを切替えながら、行列値演算を複数回繰り返すことによって生成される。

送信データ暗号化モードでは、バッファメモリの Tx-BUF 領域から３２ビットのサブブロック単位で読み出した送信データを B-REG ２０３に供給し、送信データ暗号化に必要な部分行列値をメモリ５０から M-REG ５１にロードして、積和演算部４０を起動する。この場合、B-REG ２０３に設定された１つのデータブロックに対して、M-REG ５０の内容を切替えながら、複数回の積和演算が繰り返される。

積和演算部４０の演算結果は、C-REG レジスタ２０４に出力される。C-REG レジスタ２０４に出力された演算結果は、C-MEM ５２に中間演算値として保持される。C-MEM ５２は、ＥＣＣ符号長に応じたビット数の記憶容量を有し、積和演算サイクル毎に、EOR 加算回路５３によって、新たな演算結果が部分行列と対応した中間演算値に加算される。

ＥＣＣ符号長に相当する複数サブブロック分の送信データについて暗号化演算処理が完了すると、C-MEM ５２の内容が暗号化データとして読み出され、バッファメモリ２６の Tx-ENC 領域２６２Ａに転送される。

上述した積和演算の繰り返しによって、Tx-BUF 領域に格納された１メッセージ分の暗号化処理が完了すると、動作モードが送信データ誤り符号化モード（ＣＲＣ演算モード）に切り替えられる。

送信データ誤り符号化モードでは、MAT-MWO ５０から M-REG ５１にＣＲＣ用の行列値をロードした状態で、バッファメモリ２６の Tx-ENC 領域２６２Ａから、３２ビット単位で暗号化データブロックを読み出し、B-REG レジスタ２０３と送信部１１に転送する。但し、送信データが暗号化を必要としない場合は、バッファメモリ２６の Tx-BUF 領域２６１Ａから読み出されたデータブロックが B-REG レジスタ２０３と送信部１１に供給される。

積和演算部４０は、B-REG レジスタ２０３のデータブロックと M-REG ５１が示すＣＲＣ用行列値との積和演算を実行し、演算結果を C-REG レジスタ２０４に出力する。この場合、C-REG レジスタ２０４に出力された演算結果は、既に供給済みのデータブロックに付加すべきＣＲＣ符号として、バス２９を介して送信部１０に転送される。

受信データ誤り検出モードでは、バッファメモリ２６の Rx-CRC 領域２６３Ｂから読み出した受信データを対象として、積和演算部４０により、B-REG レジスタ２０３のデータブロックと M-REG ５１のＣＲＣ用行列値との積和演算を実行する。

この場合、Rx-CRC 領域２６３Ｂには、３２ビットのデータブロック毎に３２ビットのＣＲＣ符号ブロックを付加した形で、受信データが格納されている。従って、受信データの誤りの有無は、例えば、第１サイクルで３２ビットのデータブロックを読み出してＣＲＣ:r(x)を生成し、第２サイクルで、上記データブロックに続く３２ビットのＣＲＣ符号ブロックを読み出してＣＲＣ:r'(x)を生成し、r'(x)と r(x)の一致を確認することによって判定できる。

上記 r'(x)と r(x)との一致検出は、一致検出回路５４で行われ、検出結果が制御部７０に通知される。制御部７０は、誤り検出を終えたデータブロックをバッファメモリの Rx-ENC 領域２６２Ｂ（非暗号化データブロックの場合は Rx-BUF 領域２６１Ｂ）に転送し、誤りのあるデータブロックは廃棄する。

暗号データ復号化モードでは、Rx-ENC 領域２６２Ｂから読み出したデータブロックを対象として、積和演算部４０で送信データ暗号化モードと同様の演算を行う。復号化されたデータは、C-MEM ５２から Rx-BUF 領域２６１Ｂに転送される。

第５図は、行列値演算部３０で生成される行列Mの１例を示す。

第４図の実施例では、行列値演算部３０が３２×３２サイズの行列を生成するものとして説明したが、ここでは、簡単化のために、８×８の行列を示す。b_0～b_7は、B-REG ２０３に設定されるデータビット、c_0～c_7は、演算結果としてC-REG ２０４に出力されるＣＲＣまたはＥＣＣのビットを示している。

行列Ｍの第１列の値（m_{00}～m_{70}）は、多項式a(x)の各ビットの値（a_0～a_7）で決まる。

第２列以降の値（m_{01}～m_{77}）は、基本的には

$$m(i,j)=m(i-1,j-1)+g(i)m(0,j) \qquad (14)$$

の関係にあり、各列の第１行目の値（m_{01}、m_{02}、m_{03}･･･m_{07}）は、

$$m(0,j)=g(0)m(max,j-1) \qquad (15)$$

の関係にある。ここで、m(max, j-1)は、第 j-1 列の最終行の行列値を意味している。

ここで、多項式g(x)の値は、規格で定められた固定値となる。また、ＥＣＣ暗号化／復号化の場合、多項式a(x)は暗号鍵であり、或る期間内では固定の値（半固定値）となる。また、誤り検出の場合に、a(x)に代えて使用される多項式g'(x)は、完全な固定値である。従って、これらのパラメータから生成される行列Ｍは、固定または半固定値となるため、行列値演算部３０で一度算出しておけば、演算結果を繰り返して利用できる。

行列演算部３０と積和演算部４０の行列演算能力は、ハードウェアの制約から、例えば、１６×１６または３２×３２のように限られたサイズ（以下、基本サイズと言う）となる。基本サイズより大きいｎ×ｎサイズの行列Ｍを扱うためには、行列Ｍを基本サイズをもつ複数の部分行列に分割し、部分行列毎の演算動作を繰り返す必要がある。

第６図は、ｎ×ｎの行列Ｍを部分行列Ｍ(0,0)～Ｍ(I,J)に分割した

例を示す。

ここで、例えば、最初の部分行列M(0,0)における第２列（データビットｂ$_1$列）の第１行（演算結果ｃ$_0$の行）の行列値ｍ(0,1)は、行列Mの左下に位置した部分行列M(I,0)における第１列（データビットｂ$_0$の列）の最終行の行列値ｍ(n-1,0)に依存している。図面では省略されている次の部分行列M(1,0)における第２列第１行の行列値ｍ(k,1)は、上記最初の部分行列M(0,0)における第１列最終行の行列値ｍ(k-1,0)に依存している。また、行列M全体における第１列（データビットｂ$_0$の列）を除いて、各列では、行列Mの第１行目（演算結果ｃ$_0$の行）の値が後続する全ての行（演算結果ｃ$_1$～ｃ$_{n-1}$の行）に反映されている。

従って、行列演算部３０で部分行列毎に行列値を生成する場合は、これらの境界条件を考慮したパラメータ設定が必要となる。

第７図は、１６０×１６０ビットの行列を３２×３２の基本サイズをもつ複数ブロックに分割した場合の部分行列M(0,0)～M(4,4)の配列と、入力データ（B01～B159）、出力符号(C01～C159)の関係を示す。

このような部分行列を扱う場合、積和演算部４０には、入力データ（B01～B159）が３２ビット単位のデータブロック D-0～D-4 分割した形で入力され、出力符号(C01～C159)が３２ビット単位の符号ブロック ECC-0～ECC-4 に分割した形で出力されることになる。

第８図は、ＥＣＣ行列値を３２×３２ビットの部分行列毎に生成するようにした行列値演算部３０の１実施例を示す。

行列値演算部３０は、A-REG ２０１および G-REG ２０２の各ビットと対応して用意された複数のＡＮＤ回路３１－ｉ、第１のセレクタ群３３－ｉおよび排他論理和(EOR)回路３２－ｉ（ｉ＝０～ｋ、ｋ＝３１）と、これらの EOR 回路の出力値を保持するための複数ビットの記憶領域３５－ｉ（ｉ＝０～ｋ）をもつレジスタ３５とからなる。

EOR回路３２－ｉの第１入力には、制御部７０からの制御信号Ｓ０で制御されるセレクタ３３－ｉを介して、A-REG ２０１の第ｉビットの値ａｉとＡＮＤ回路３１－ｉの出力値の何れかが選択的に供給される。最初のEOR回路３２－０を除いて、EOR回路３２－ｉ（ｉ＝１～ｋ）には、レジスタ３５に保持された前列前行の行列値m(i-1, j-1)が第２入力として供給される。最初のEOR回路３２－０の第２入力には、制御部７０からの制御信号Ｓ２で制御されるセレクタ３７を介して、固定値“０”またはレジスタ３５の最終ビット記憶領域３５－ｋに保持された前列最終行の行列値m(31, j-1)が供給される。

セレクタ３３－０から出力される部分行列第１行目の行列値は、制御部７０からの制御信号Ｓ３で指定される所定のタイミングで、ラッチ回路３４に保持される。

ＡＮＤ回路３１－ｉには、G-REG ２０２の第ｉビットの値ｇｉが第１入力として供給される。最初のＡＮＤ回路３１－０の第２入力には、セレクタ３６－０を介して、前列最終行の行列値m(31, j-1)と上記ラッチ回路３４に保持された部分行列第１行目の行列値の何れかが供給される。他のＡＮＤ回路３１－ｉ（ｉ＝１～ｋ）の第２入力には、セレクタ３６－ｉを介して、セレクタ３３－０の出力値またはラッチ回路３４に保持された部分行列第１行目の行列値の何れかが供給される。セレクタ３６－０～３６－ｋは第２のセレクタ群を構成しており、制御部７０からの制御信号Ｓ１で制御される。

本実施例では、ＣＲＣ用行列演算とＥＣＣ用行列演算に共用するために、行列値演算部３０が、EOR回路３２－ｉの出力ビットを保持するためのシフトレジスタ(SHIFT)３８－ｉと、シフトレジスタ３８－ｉの出力値とレジスタ領域３５－ｉの出力値の何れかを選択して次行EOR回路３２－(ｉ＋１)に供給する第３のセレクタ群３９－ｉ（ｉ＝０～

k）を備えている。第３のセレクタ群は、制御信号S1で制御される最後のセレクタ３９－ｋを除いて、制御信号S4に応じてＡポート、Ｂポートの何れかの入力を選択する。

ＣＲＣ用の行列値を生成する場合、制御部７０は、セレクタ３７と第２セレクタ群３６－０～３６－ｋと第３のセレクタ群３８－０～３８－ｋが常時Ａポート入力を選択するように、制御信号S1、S2、S4を出力する。また、第１セレクタ群３３－０～３３－ｋが、行列Ｍの第１列目の行列値演算サイクルではＡポート入力（A-REG出力）、第２列～第ｋ列（ｋ＝３１）の行列値演算サイクルではＢポート入力（ＡＮＤ回路３１－ｉの出力）を選択するように、制御信号S0が切替えられる。

従って、第１列目の行列値演算サイクルでは、EOR回路３２－ｉ（ｉ＝０～ｋ）から、A-REG ２０１が示す各ビットの値a_0～a_{31}が生成される。これらのビット値は、レジスタ３５の各記憶領域３５－０～３５－ｋに設定された後、MAT-MEM ５０のＣＲＣ用行列領域、図示した例ではＭ（0,0）の第１列目に記憶される。

次の、第２列目の行列値演算サイクルでは、第１行目のセレクタ３３－０から、セレクタ３６－０で選択された記憶領域３５－ｋが示す前サイクル最終行の行列値a_{31}とG-REG ２０２が示す第１ビットの値g_0との間の論理積を示す値（$m_{0,1}$）が出力され、EOR回路３２－０に入力される。上記値$m_{0,1}$は、第２のセレクタ群３６－ｉ（ｉ＝１～ｋ）を介して他のＡＮＤ回路３１－ｉにも入力される。従って、第１行目以降のセレクタ３３－ｉからは「$g_i \cdot m_{0,1}$」を示す値が出力され、EOR回路３２－ｉから式（１４）が示す行列値が出力される。

第２列目～第ｋ列目の各演算サイクルで、上記と同様の演算動作を繰り返すことによって、ＣＲＣ用行列領域Ｍ（0,0）に式（１４）、（１

5）に従った行列値を生成することができる。

一方、ＥＣＣ用の行列値を生成する場合は、第３のレジスタ群３９－ｉ（ｉ＝０～ｋ）にＢポート入力を選択させた状態で、A-REG ２０１の設定パラメータを入れ替えながら、行列Ｍの第１列目の行列値演算サイクルが繰り返される。これらの演算サイクルで、レジスタ３５にa0～a31、a32～a63、…a128～a159の値が次々と生成され、部分行列Ｍ（0,0）、Ｍ（1,0）、…Ｍ（4,0）の第１列目に記憶される。

この時、最初のシフトレジスタ３８－０には、a_0、a_{32}、a_{64}、a_{96}、a_{128}のビット値が保持され、次のシフトレジスタ３８－１には、a_1、a_{33}、a_{65}、a_{97}、a_{129}のビット値、最後のシフトレジスタ３８－ｋには、a_{31}、a_{63}、a_{92}、a_{127}、a_{159}のビット値が保持された状態となる。

第１列目の行列値演算が終了すると、制御信号Ｓ０と制御信号Ｓ２によって、第１セレクタ群３３－ｉとセレクタ３７がそれぞれのＢポート入力を選択するように切替える。この時点では、レジスタ３５の記憶領域３５－ｋには、行列値$m_{31,j-1}$としてパラメータ値“a_{159}”が設定されている。

以下、G-REG ２０２の設定値を入れ替えながら、部分行列Ｍ（0,0）、Ｍ（1,0）、…Ｍ（4,0）の第１列目の行列値演算サイクルを繰り返す。

G-REG ２０２に第１ブロックのパラメータ値g_0～g_{31}を設定した演算サイクルでは、制御信号Ｓ１の切替えによって、第２セレクタ群３６－ｉと、第２セレクタ群の最後のセレクタ３９－ｋにＡポート入力を選択させ、セレクタ３３－０の出力値“$g_0 \cdot a_{159}$”を他の行のＡＮＤ回路３１－ｉに入力する。また、制御信号Ｓ３で与えるラッチ指令によって、上記セレクタ３３－０の出力値“$g_0 \cdot a_{159}$”をラッチ回路３４に記憶する。この時、EOR 回路３２－ｊには、シフトレジス

タ３８－(j-1)から出力された前列前行のビット値m(0, j-1)が入力されるため、式（１４）、（１５）に従った第２行目の行列値$m_{0,1}$～$m_{31,1}$が生成され、これらの値が、シフトレジスタ３８－０～３８－ｋとMAT-MEM５０のＥＣＣ用部分行列M(0, 0)の第２列目に記憶される。

G-REG２０２に第１ブロック（g_{32}～g_{63}）～第４ブロック（g_{127}～g_{159}）のパラメータ値を設定した状態で行われる各演算サイクルでは、制御信号Ｓ１との切替えによって、第２セレクタ群３６－ｉと、第３セレクタ群の最後のセレクタ３８－ｋにＢポート入力を選択させる。すなわち、部分行列M（1, 0）～M（4, 0）の行列値に、上記ラッチ回路３４に記憶された“$g_0 \cdot a_{159}$”を反映させる。これによって、式（１４）、（１５）に従った第１行目の行列値（$m_{32,1}$～$m_{63,1}$）～（$m_{127,1}$～$m_{159,1}$）が次々と生成され、MAT-MEM５０の部分行列M（1, 0）～M（4, 0）の第２列目に記憶される。

部分行列M（0, 0）、M（1, 0）、…M（4, 0）の第３列目～第３２列目の行列値は、上述した第２列目と同様の手順を繰り返すことによって生成でされる。残りの部分行列M（0, 1）、M（1, 1）、…M（4, 4）では、第１列から第３２列までの全ての行列値演算にG-REG２０２の設定値を利用し、部分行列M（0, 0）、M（1, 0）、…M（4, 0）の第２列目以降の演算サイクルと同様の手順を繰り返す。

第９図は、第８図に示した行列値演算部３０を制御対象として制御部７０が実行するＣＲＣ行列値生成ルーチン１００の１実施例を示す。

ＣＲＣ行列値生成ルーチン１００では、列を指定するためのパラメータｉを初期値０、最後の列を示すパラメータjmaxの値を「３１」に設定(ステップ１０１)した後、メモリ領域２７１から読み出したg'-CRCの値をA-REG２０１とG-REG２０２にロードする（ステップ１０２、１０３）。次に、制御信号S1～S4の発生パターンを単一行列モ

ードに設定する。ここで、単一行列モードは、行列値の演算が基本サイズ３２×３２ビットの単一の部分行列で完了することを意味しており、このモードでは、制御信号S1、S2、S4は、第２、第３のセレクタ群３６－ｉ、３９－ｉ（ｉ＝０～ｋ）とセレクタ３７に常時Ａポート入力を選択させた状態となり、制御信号S3は、ラッチ信号を全く発生しない状態となる。

先ず、制御信号S0によって、第１セレクタ群３３－ｉ（ｉ＝０～ｋ）にA-REG ２０１の出力（Ａポート入力）を選択させ（１０５）、EOR回路３２－ｉ（ｉ＝０～ｋ）により第ｊ列の行列値を演算する（１０６）。EOR回路から出力された第ｊ列の演算結果は、レジスタ３５に保持した後、MAT-MEM ５０に定義されたＣＲＣ用の行列領域に記憶する（１０７）。制御信号S0の状態を切替えて、第１セレクタ群３３にG-REG ２０２の出力（Ｂポート入力）を選択させる（１０８）。

次に、パラメータｊの値をインクリメントし（１０９）、ｊの値をjmaxと比較する（１１０）。ｊ＞jmaxとなっていた場合は、このルーチンを終了し、そうでなければ、パラメータｊが示す次列の行列値をEOR回路３２－ｉにより演算し（１１１）、第ｊ列の演算結果をＣＲＣ用の行列領域に記憶する（１１２）。この後、ステップ１０９に戻り、ｊ＞jmaxとなる迄、同様の動作を繰り返す。

ＣＲＣ用の行列Ｍのサイズは、行列値演算部３０が扱う基本サイズとなっているため、上述したように、ｊ＝０～jmaxの行列値の演算を繰り返すことによって、積和演算部４０が必要とする全ての行列値を生成できる。

第１０図は、第８図に示した行列値演算部３０を制御対象として制御部７０が実行するＥＣＣ行列値生成ルーチン１２０の１実施例を示す。

ＥＣＣ行列値生成ルーチン１２０では、図７に示した部分行列Ｍ(I,J)を特定するためのパラメータＩ、Ｊの値と、部分行列Ｍ(I,J)内での列番号を指定するためのパラメータｊの値を初期値０に設定し、パラメータＩとＪの最大値 Imax と Jmax を４、ｊの最大値 jmax を３１に設定する（１２１）。

次に、制御信号 S1、S2、S3、S4 の発生パターンを部分行列モードに設定する。ここで、部分行列モードは、行列値の演算が複数の部分行列に分割して実行されることを意味しており、このモードでは、制御信号 S1 は、第２セレクタ群３６－ｉ（ｉ＝０～ｋ）とセレクタ３９－ｋが、部分行列Ｍ(0,J)の演算サイクルではＡポート入力、その他の部分行列Ｍ(I,J)（但し、Ｉ＝１～４）の演算サイクルではＢポート入力を選択するように切替えられ、制御信号 S2 は、セレクタ３７が、部分行列Ｍ(I,0)（但し、Ｉ＝0～４）の第１列の演算サイクルではＡポート入力、その後はＢポート入力を選択するように切替えられる。

また、制御信号 S3 は、部分行列Ｍ(0,J)の各列の演算サイクルでラッチ信号を発生し、ラッチ回路３４にセレクタ３３－０の出力値を保持させる。ラッチ回路３４の出力値は、部分行列Ｍ(１,J)～Ｍ(4,J)の演算サイクルでは不変となる。制御信号 S4 は、第３セレクタ群３９－ｉ（ｉ＝０～ｋ－１）に常時、Ａポート入力を選択させる。

先ず、制御信号 S0 によって、第１セレクタ群３３－ｉ（ｉ＝０～ｋ）に A-REG ２０１の出力（Ａポート入力）を選択させ（１２３）、メモリ２７の E-KEY 領域２７３から A-REG ２０１に暗号鍵の第Ｉブロック KEY(I)をロードする（１２４）。この時、EOR 回路３２－ｉ（ｉ＝０～ｋ）は、KEY(I)が示す３２ビットのパラメータに従って、部分行列Ｍ(I,J)の第１列の行列値を演算する（１２５）。この演算結果は、シフトレジスタ３８とレジスタ３５に保持した後、MAT-MEM ５０に定義され

たＥＣＣ用部分行列領域M(I,J)の第ｊ列に記憶される（１２６）。

次に、パラメータＩの値をインクリメントし（１２７）、Ｉの値をImaxと比較する（１２８）。Ｉ＞Imaxでなければ、ステップ１２４に戻って、E-KEY領域２７３から暗号鍵の次のブロックKEY(I)をA-REG２０１にロードし、同様の動作を繰り返す。

Ｉ＞Imaxとなった場合は、制御信号S0の状態を切替えて、第１セレクタ群３３にG-REG２０２の出力（Ｂポート入力）を選択させ（１３０）、パラメータＩを初期値０に戻し、パラメータｊの値をインクリメントする（１３３）。

次に、パラメータｊの値をjmaxと比較し（１３４）、ｊ＞jmaxでなければ、メモリ２７のｇ-ECC領域２７２からA-REG２０１に多項式ｇ(x)の第Ｉブロックｇ-ECC(I)をロードする（１３５）。これによって、EOR回路３２－ｉ（ｉ＝０～ｋ）で、ｇ-ECC(I)が示す３２ビットのパラメータに従った部分行列M(I,J)の第ｊ列の行列値が演算される（１３６）。演算結果は、レジスタ３５に保持した後、MAT-MEM５０に定義されたＥＣＣ用部分行列領域M(I,J)の第ｊ列に記憶される（１３７）。

次に、パラメータＩの値をインクリメントし（１３８）、Ｉの値をImaxと比較する（１３９）。Ｉ＞Imaxでなければ、ステップ１３５に戻って、E-KEY領域２７３からｇ(x)の次のブロックｇ-ECC(I)をA-REG２０１にロードし、同様の動作を繰り返す。ステップ１３９でＩ＞Imaxとなった場合は、ステップ１３３に戻り、パラメータＩを初期値０に戻し、パラメータｊの値をインクリメントして、次列の行列値について上記と同様の手順を繰り返す。

ステップ１３４でｊ＞jmaxとなった場合、ステップ１４０に進み、パラメータｊとＩの値を初期値０に戻し、パラメータＪの値をインクリメントする。これによって、次列の部分行列M(I,J)が演算対象とな

る。パラメータＪの値をJmaxと比較し（１４１）、Ｊ＞Jmaxとなっていた場合は、このルーチンを終了する。Ｊ＞Jmaxでなければ、ステップ１３５に進む。これによって、部分行列Ｍ(0,J)～Ｍ(4,J)内の第１列から第３２列について、上述した行列値の演算動作が繰り返される。

尚、上記ステップ１３３～１４１の実行過程で、部分行列Ｍ(0,J)の各列の演算サイクルで、制御信号S3で与えるラッチ指令によって、行列Ｍの第１行目の行列値がラッチ回路３４に保持され、この値が後続する部分行列Ｍ(1,J)～Ｍ(4,J)の各演算サイクルでＡＮＤ回路３１－０～３１－ｋに供給される。また、第８図に示した第１行のEOR回路３２－０には、レジスタ３５の最後の記憶領域３５－ｋから出力される前列最終行の行列値が供給されているため、第６図で説明した部分行列間の境界条件を満たすことができる。

以上、ＥＣＣ暗号化用の行列値生成ルーチンについて説明したが、ブロックKEY(I)として、メモリ２７のD-KEY領域から読み出した復号鍵を適用すれば、ルーチン１２０と同様の制御手順でＥＣＣ復号化用の行列値を生成できる。

第１１図の（Ａ）と（Ｂ）は、積和演算部４０を制御対象として制御部７０が実行する送信データ処理ルーチン２００と受信データ処理ルーチン３００のフローチャートを示す。

送信データ処理ルーチン２００は、バッファメモリ２６のTx-BUF領域２６１Ａから読み出した送信データ（送信メッセージ）の暗号化処理（２１０）と、Tx-ENC領域２６２Ａから読み出した暗号化データについてのＣＲＣ生成／送信処理（２３０）とからなる。但し、送信データの暗号化が不要の場合は、Tx-BUF領域２６１Ａから読み出した送信データを処理対象として、ＣＲＣ生成／送信処理（２３０）が実行される。

一方、受信データ処理ルーチン３００は、バッファメモリ２６のRx-CRC領域２６３Ｂに蓄積された受信データについてのＣＲＣ生成処理（３１０）と、ＣＲＣチェック（３２０）の結果、誤りなしと判定された受信データを対象とした復号化処理（３３０）とからなる。復号化処理（３３０）では、受信データが暗号化データか否かを判定し、暗号化データでなければ、受信データをそのままRx-BUF領域１６１Ｂに転送し、暗号化データの場合には、これを復号化した後、Rx-BUF領域１６１Ｂに転送する。ＣＲＣチェックの結果、誤りが検出された受信データについては、例えば、上位装置であるコアプロセッサ１０へのエラー通知などのエラー処理（３５０）が実行される。

上記送信データ処理ルーチン２００と受信データ処理ルーチン３００は、メッセーシ単位で交互に実行される。

第１２図は、送信データの暗号化処理２１０の１実施例を示すフローチャートである。

制御部７０は、Tx-BUF領域２６１Ａから送信メッセージのヘッダ部を読み出し（２１１）、ヘッダ部が示すデータ長Ｌから、送信データを暗号化データのブロック長、この例では１６０ビット単位で分割した場合のブロック数Nmaxを計算し、暗号化処理の繰り返し回数を示すパラメータｎの値を初期値１に設定する（２１２）。本実施例では、ヘッダ部は暗号化の対象外とし、Tx-ENC領域２６２Ａに転送する（２１３）。

先ず、部分行列M(I,J)を指定するためのパラメータＩ、Ｊの値を初期値０に設定し（２１４）、Tx-BUF領域２６１Ａから、送信データのｎ番目のデータブロックを３２ビット単位で読み出し、B-REG ２０３に転送する（２１５）。ここでは、B-REG ２０３に読み出された３２ビットのデータブロックをD(n)-Jで表す。最初に読み出されたデータブロ

ックD(n)-0は、第７図におけるデータD-0に相当し、その次に読み出されるデータブロックD(n)-1は、データD-1に相当する。

次に、メモリ５０からM-REG ５１に暗号化用の部分行列M(I,J)をロード（２１６）し、積和演算部４０を起動すると（２１７）、C-REG ２０４に部分行列M(I,J)とデータD(n)-Jとの積和演算結果が出力される。部分行列M(0,0)を使用した最初の積和演算では、第７図に示したC0～C31の値が求まる。この値は、ＥＣＣ符号の部分計算値に過ぎないため、C-MEM ５２のECC-I領域の既演算値にＥＯＲ加算する（２１８）。C-MEM ５２には、部分行列M(I,J)のパラメータＪと対応して、３２ビット長の符号値記憶領域ECC-0～ECC-4が用意してあり、各領域の初期値は０となっている。

パラメータＩの値をインクリメントし（２１９）、Ｉ＞４か否かを判定する（２２０）。Ｉの値が４以下であれば、ステップ２１６に戻り、上述した動作を繰り返す。これによって、データD-0と部分行列M(１,0)～M(４,0)の積和演算が次々と実行され、演算結果C32-C63～C128-C159がC-MEM ５２のECC-1～ECC-4の既演算値にＥＯＲ加算される。

パラメータＩをインクリメントした結果、Ｉ＞４となった場合は、Ｉの値を初期値０に戻し、Ｊの値をインクリメントして（２２１）、Ｊ＞４か否かを判定する（２２２）。Ｊの値が４以下の場合は、ステップ２１５に戻って、Tx-BUF領域２６１ＡからB-REG ２０３に、送信データの次のブロックD(n)-Jを転送し、ステップ２１５～２２２の動作を繰り返す。Ｊの値が４を超えるまで、上述した動作を繰り返すことによって、第７図に示したデータD-1と部分行列M(0,1)～M(4,1)、データD-2と部分行列M(0,2)～M(4,2)、データD-3と部分行列M(0,3)～M(4,3)、データD-4と部分行列M(0,4)～M(4,4)の積和演算が次々と

実行され、各積和演算の結果がC-MEM ５２のECC-0～ECC-4に次々とＥＯＲ加算される。

パラメータＪの値がＪ＞４となった時、C-MEM ５２の内容（ECC-0～ECC-4）は、１６０ビット長送信データについての暗号化結果を示している。従って、C-MEM ５２の内容をバッファメモリのTx-ENC領域２６２Ａに転送し（２２３）、C-MEM ５２のECC-0～ECC-4をクリア（２２４）した後、パラメータｎの値をインクリメントする（２２５）。ｎの値を最大値Nmaxと比較し（２２６）、ｎ＞Nmaxでなければ、ステップ２１４に戻って、次の１６０ビット長の送信データD(n)を対象として、暗号化処理を繰り返す。ｎ＞Nmaxとなった時点で、１つの送信メッセージの暗号化が完了する。

第１３図は、ＣＲＣ生成／送信処理（２３０）の１実施例を示すフローチャートである。

ＣＲＣ生成／送信処理（２３０）では、Tx-ENC領域２６.２Ａから３２ビット単位で暗号化データを読み出して、ＣＲＣを生成する。ここでは、暗号化された送信データを対象として説明するが、送信メッセージを暗号化することなく送出する場合は、Tx-BUF領域２６１Ａのデータをの生成対象とすればよい。

先ず、Tx-ENC領域２６２Ａから送信メッセージのヘッダ部を読み出し、送信部１１に転送する（２３１）。次に、暗号化データの長さＫを３２ビット単位で読み出した場合のデータブロック数Nmaxを計算し、処理の繰り返し回数を示すパラメータｎの値を初期値“１”に設定する（２３２）。

メモリ５０からM-REG ５１にＣＲＣ用の行列値Ｍをロード（２３３）した後、Tx-ENC領域２６２Ａから暗号化送信データの最初のデータブロックD(n)を読み出し、送信部１１とB-REG ２０３に転送する（２３

４）。この状態で積和演算部４０を起動すると（２３５）、C-REG ２０４にＣＲＣ用行列Ｍとデータ D(n)との積和演算結果 C0～C31 が出力される。

ＣＲＣ生成の場合、積和演算部４０の一回の起動でデータブロック D(n)に付加すべきＣＲＣ符号が生成できるため、C-REG ２０４の内容を送信部１１に送信し（２３６）、パラメータｎの値をインクリメントして（２３７）、ｎの値を Nmax と比較する（２３８）。ｎが Nmax 以下の場合はステップ２３４に戻って、Tx-ENC 領域２６２Ａから次のデータブロック D(n)を読み出し、上述した動作を繰り返し、ｎ＞Nmax となった時、１メッセージ分のＣＲＣ生成処理を終了する。

第１１図に示した受信データ処理ルーチン３００におけるＣＲＣ生成処理３１０は、第１３図で説明した送信データのＣＲＣ生成ルーチンにおいて、読み出すべきデータブロックの記憶領域を Tx-ENC 領域２６２Ａから Rx-CRC 領域２６３Ｂに変更し、ヘッダとデータブロックとＣＲＣの転送先を送信部１１からバッファメモリの Rx-ENC 領域２６２Ｂ（平文受信データの場合は Tx-BUF 領域２６１Ｂ）に変更すればよい。

また、受信データの復号化処理３３０は、Rx-ENC 領域２６２Ｂから読み出したデータブロックをメモリ５０から M-REG ５１にロードした復号化用の部分行列で積和演算処理すればよいため、基本的には、第１２図で説明した送信データ暗号化ルーチンと同様の手順となる。

以上の実施例では行列値演算部３０で生成したＣＲＣ用、ＥＣＣ用の行列をメモリ（MAT-MEM）５０に格納しておき、ＣＲＣ生成とＥＣＣ暗号化／復号化処理を行う時、積和演算部４０が必要とする行列の値を MAT-MEM ５０から M-REG ５１に適宜ロードするようにしたが、M-REG ５１をＣＲＣ用、ＥＣＣ暗号化用、復号化用の専用レジスタとして用意しておき、行列値演算部３０で生成した行列値をこれらの専用レジ

スタに直接ロードするようにしてもよい。この場合、積和演算部４０に接続すべきM-REG ５１を切替えることによって、ＣＲＣ生成とＥＣＣ暗号化／復号化処理を高速に行うことが可能になる。

また、実施例では、行列値演算部で生成する行列の基本サイズを３２×３２としたが、これを８×８、または１６×１６のように小型化した場合、ＣＲＣ用の行列も部分行列モードで生成することになる。この場合、ＣＲＣ行列値生成ルーチン１００に、第１０図で説明したＥＣＣ行列値生成ルーチン１２０と同様の制御手法を採用すればよい。

本発明によれば、予め用意した行列値を利用することによって、送受信データの誤り検出に必要なＣＲＣ符号を高速に生成できる。また、ＣＲＣ用の行列を生成する行列値演算部を利用して、ＥＣＣ暗号化用および復号化用の行列値を迅速に生成できる。従って、安全性を高めるために暗号鍵を適宜変更したい場合に、外部から暗号鍵データを与えて、制御部７０にＥＣＣ行列生成ルーチンを実行させることにより、暗号鍵に応じた新たな行列値を容易に生成することが可能となる。

産業上の利用可能性

本発明によれば、誤り検出符号生成と暗号化処理にハードウェア（行列値演算部と積和演算部）を共用できるため、コンパクトなパケット通信装置を提供できる。また、暗号化／復号化処理に必要な行列値をパケット通信装置内で生成できるため、暗号鍵変更が容易であり、送受信データの安全性を向上できる。

請　求　の　範　囲

１．それぞれ所定ビット長のパラメータが設定される第１、第２レジスタ（２０１、２０２）と、符号化すべきデータが設定される第３レジスタ（２０３）と、上記第１、第２レジスタの設定値から行列値を生成する行列値演算部（３０）と、上記行列値演算部で生成された行列値を保持する行列値レジスタ（５１）と、上記行列値レジスタが保持する行列値と上記第３レジスタに設定されたデータとの積和演算を実行する積和演算部（４０）とを有し、

上記第１、第２レジスタの設定パラメータを変えることによって、上記行列値演算部で誤り検出用の行列値と暗号化用の行列値を選択的に生成し、上記行列値レジスタに保持する行列値を切替えることによって、上記積和演算部で誤り符号化演算と暗号化演算を選択的に行うことを特徴とする符号演算装置。

２．少なくとも一方にｎ次多項式の係数値データが設定される第１、第２レジスタ（２０１と２０２）と、符号化すべきデータが設定される第３レジスタ（２０３）と、上記第１、第２レジスタの設定値からｎ×ｎの行列値を生成する行列値演算部（３０）と、上記行列値演算部で生成された行列値を保持する行列値レジスタ（５１）と、上記行列値レジスタが保持する行列値と上記第３レジスタに設定されたデータとの積和演算を実行する積和演算部（４０）とを有し、

上記第３レジスタに送信データまたは受信データを供給することによって、上記積和演算部から符号化データを得るようにしたことを特徴とする符号演算装置。

３．前記行列値演算部で誤り検出用の行列値を生成し、前記積和演算部から前記第３レジスタの設定データと対応する誤り検出符号を得る

ことを特徴とする請求項２に記載の符号演算装置。

４．前記第１、第２レジスタに、ガロア体のｎ次の多項式ｇ(ｘ)の最高次ｎの係数を除いた係数データ（ｇ'）を設定し、前記積和演算部から、前記第３レジスタの設定データに対する多項式ｇ(ｘ)を法（ｍｏｄ）とするＣＲＣ符号を得ることを特徴とする請求項３に記載の符号演算装置。

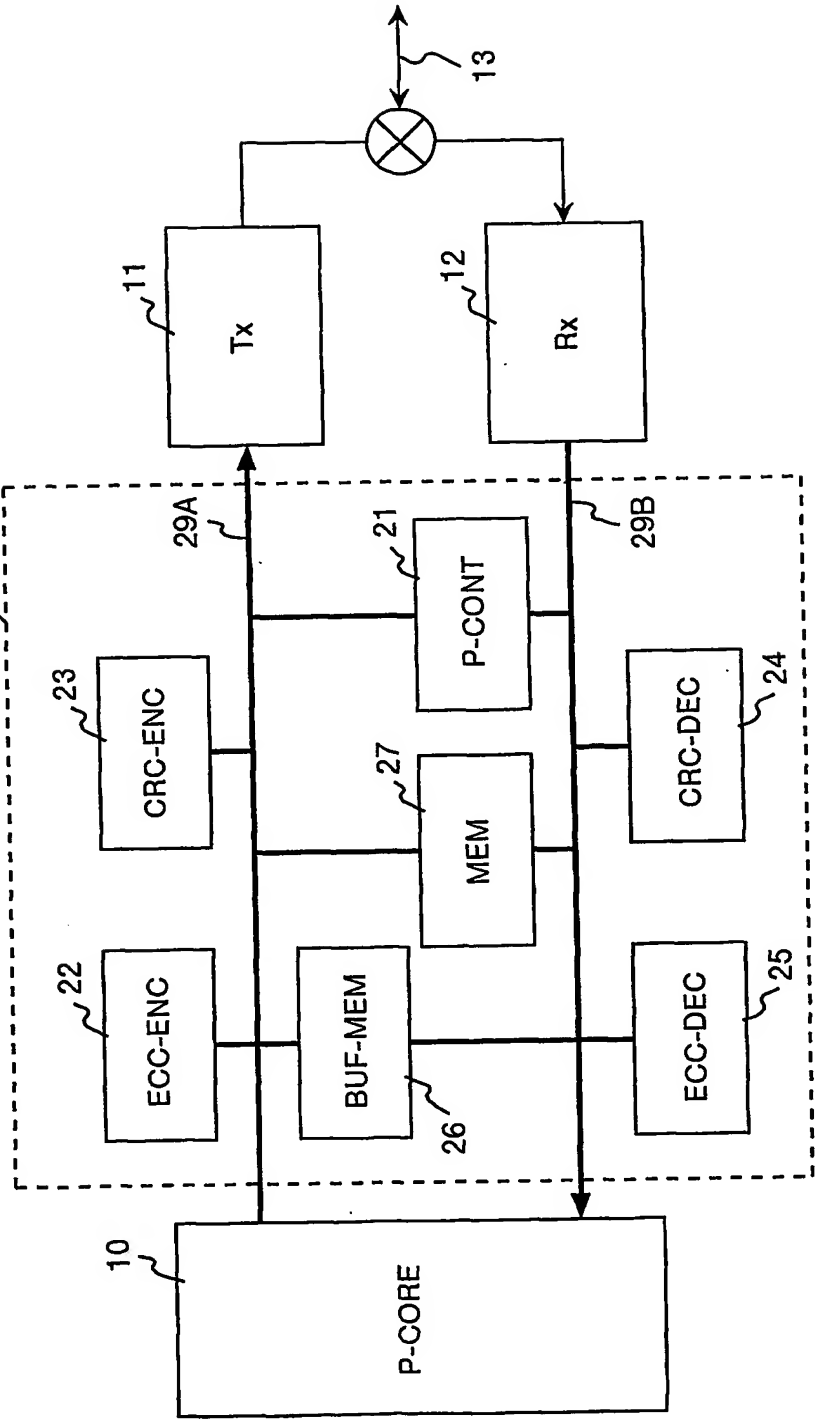
５．前記行列値演算部で暗号化用の行列値を生成し、前記積和演算部から前記第３レジスタの設定データの暗号化符号を得ることを特徴とする請求項２に記載の符号演算装置。

６．ガロア体のｎ次既約多項式ｇ(x)の係数データと暗号鍵データを記憶するための第１メモリと、上記メモリから係数データと暗号鍵データをそれぞれ複数のデータブロックに分割して読み出し、前記第１、第２レジスタに設定する制御部（７０）と、複数の部分行列値を記憶するための第２メモリとを備え、

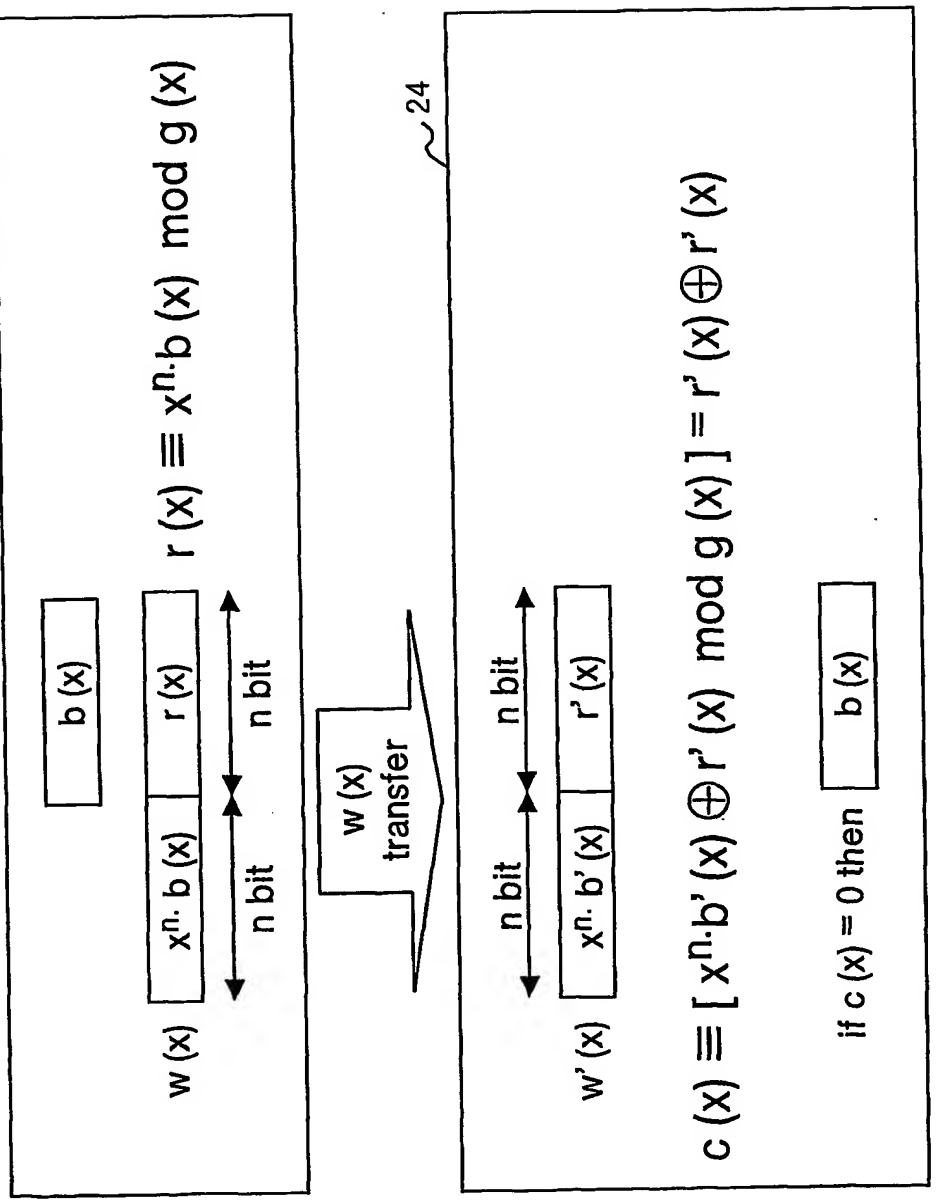
前記行列値演算部（３０）でｎ×ｎの複数の部分行列値を生成し、上記制御部の制御の下で、上記行列値演算部で生成された部分行列値を上記第２のメモリに記憶しておき、上記第２のメモリから前記行列値レジスタ（５１）に部分行列値を選択的にロードし、前記積和演算部で前記第３レジスタの設定データと複数の部分行列値との積和演算を繰り返すことによって、前記暗号化符号を得ることを特徴とする請求項５に記載の符号演算装置。

７．前記積和演算部で生成された積和演算結果を中間演算値として保持されている既演算値に排他的論理和加算し、新たな中間演算値として保持するための手段を（５２、５３）有することを特徴とする請求項６に記載の符号演算装置。

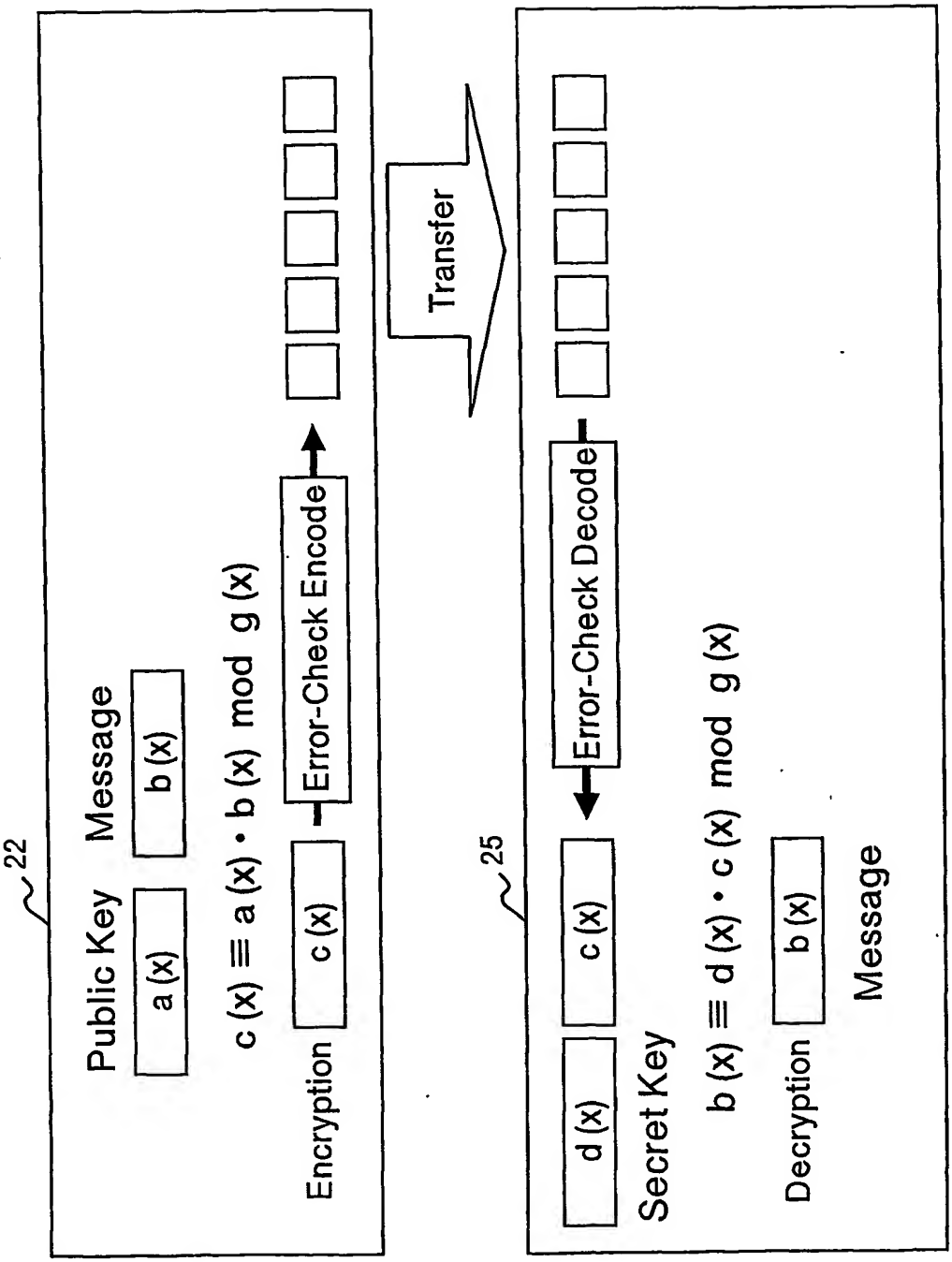
第1図


13
11
Tx
12
Rx
20
29A
29B
21
P-CONT
23
CRC-ENC
24
CRC-DEC
27
MEM
22
ECC-ENC
BUF-MEM
26
ECC-DEC
25
10
P-CORE

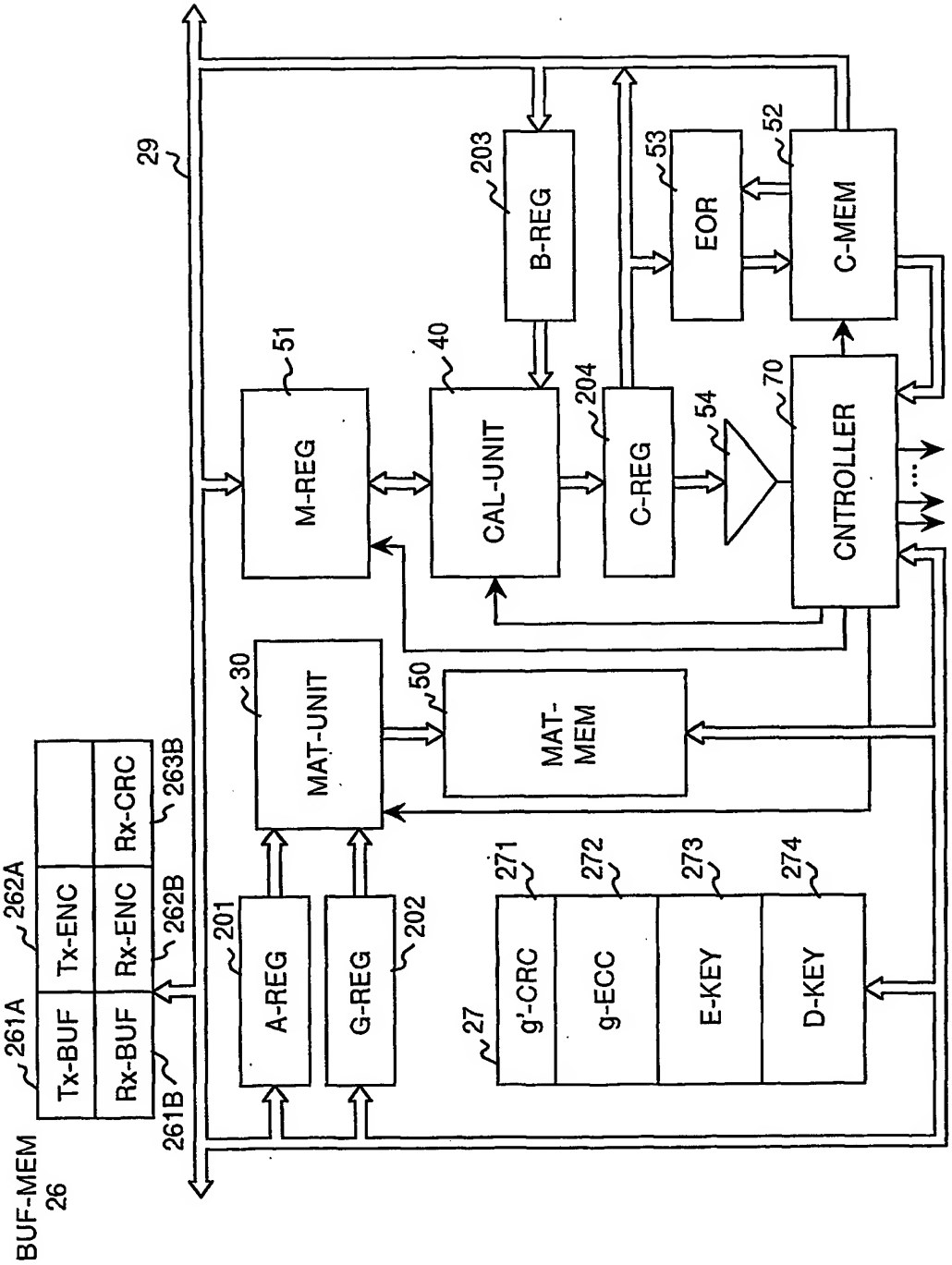
第2図


23
b (x)
r (x) ≡ x^n·b (x) mod g (x)
w (x)
x^n· b (x)
r (x)
n bit
n bit
w (x) transfer
24
n bit
n bit
w' (x)
x^n· b' (x)
r' (x)
c (x) ≡ [x^n·b' (x) ⊕ r' (x) mod g (x)] = r' (x) ⊕ r' (x)
if c (x) = 0 then
b (x)

第３図


22
Public Key
a (x)
b (x)
Message
c (x) ≡ a (x) • b (x) mod g (x)
Encryption
c (x)
Error-Check Encode
Transfer
25
Error-Check Decode
c (x)
d (x)
Secret Key
b (x) ≡ d (x) • c (x) mod g (x)
Decryption
b (x)
Message

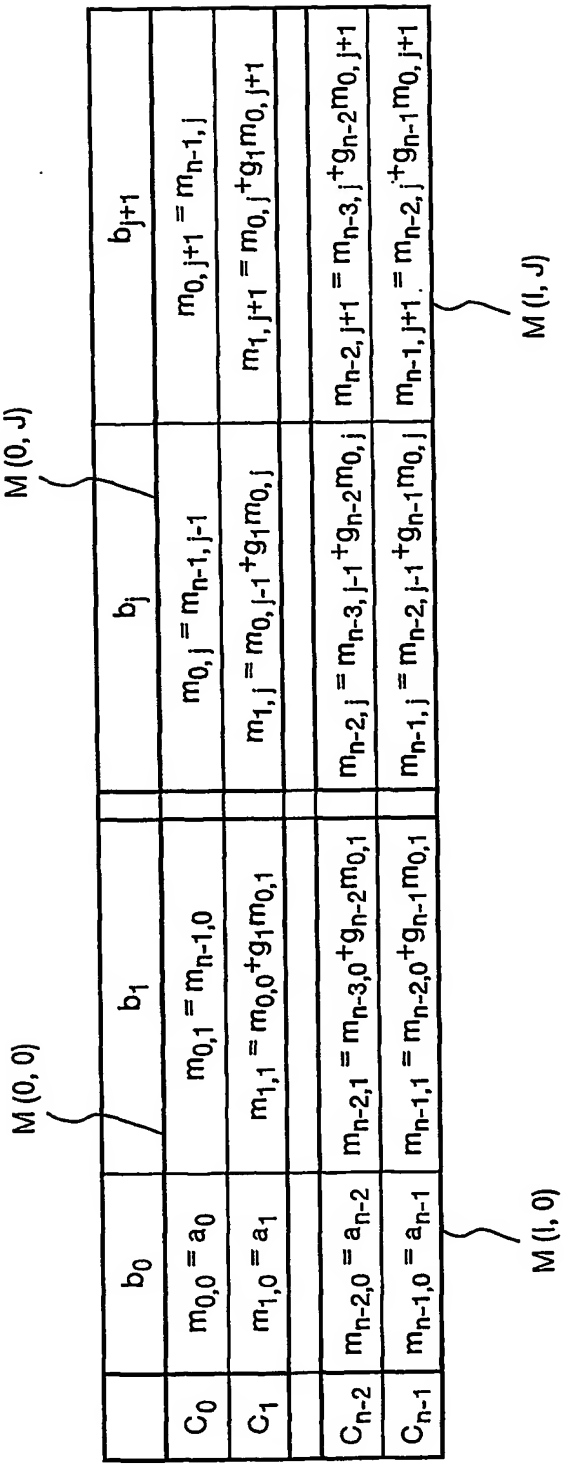
第4図


BUF-MEM
26
261A
Tx-BUF
261B
Rx-BUF
262A
Tx-ENC
262B
Rx-ENC
263B
Rx-CRC
29
201
A-REG
202
G-REG
30
MAT-UNIT
50
MAT-MEM
51
M-REG
40
CAL-UNIT
203
B-REG
204
C-REG
53
EOR
52
C-MEM
54
70
CNTROLLER
27
271
g'-CRC
272
g-ECC
273
E-KEY
274
D-KEY

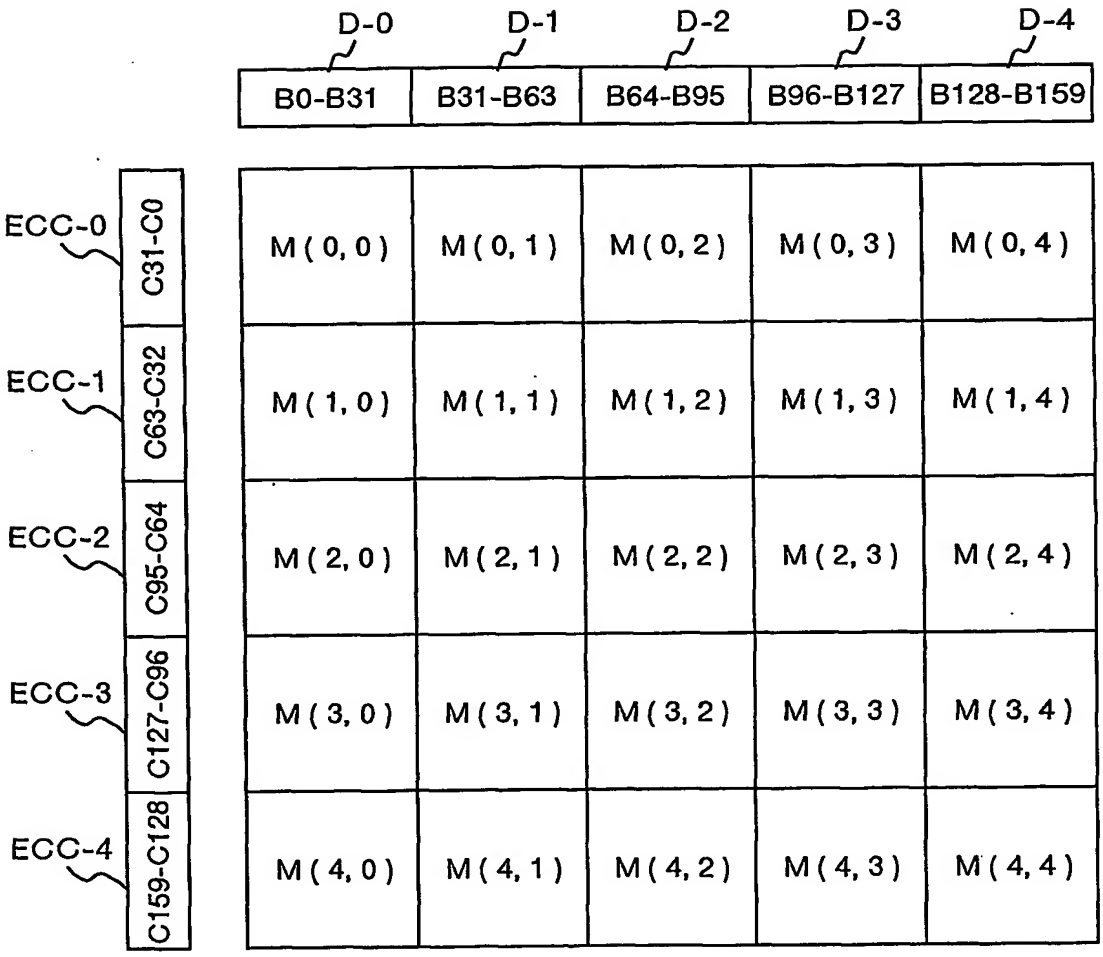
第5図

	b_0	b_1	b_2	b_3	b_4	b_5	b_6	b_7
c_0	$m_{00}=a_0$	$m_{01}=g_0m_{70}$	$m_{02}=g_0m_{71}$	$m_{03}=g_0m_{72}$	$m_{04}=g_0m_{73}$	$m_{05}=g_0m_{74}$	$m_{06}=g_0m_{75}$	$m_{07}=g_0m_{76}$
c_1	$m_{10}=a_1$	$m_{11}=m_{00}+g_1m_{01}$	$m_{12}=m_{01}+g_1m_{02}$	$m_{13}=m_{02}+g_1m_{03}$	$m_{14}=m_{03}+g_1m_{04}$	$m_{15}=m_{04}+g_1m_{05}$	$m_{16}=m_{05}+g_1m_{06}$	$m_{17}=m_{06}+g_1m_{07}$
c_2	$m_{20}=a_2$	$m_{21}=m_{10}+g_2m_{01}$	$m_{22}=m_{11}+g_2m_{02}$	$m_{23}=m_{12}+g_2m_{03}$	$m_{24}=m_{13}+g_2m_{04}$	$m_{25}=m_{14}+g_2m_{05}$	$m_{26}=m_{15}+g_2m_{06}$	$m_{27}=m_{16}+g_2m_{07}$
c_3	$m_{30}=a_3$	$m_{31}=m_{20}+g_3m_{01}$	$m_{32}=m_{21}+g_3m_{02}$	$m_{33}=m_{22}+g_3m_{03}$	$m_{34}=m_{23}+g_3m_{04}$	$m_{35}=m_{24}+g_3m_{05}$	$m_{36}=m_{25}+g_3m_{06}$	$m_{37}=m_{26}+g_3m_{07}$
c_4	$m_{40}=a_4$	$m_{41}=m_{30}+g_4m_{01}$	$m_{42}=m_{31}+g_4m_{02}$	$m_{43}=m_{32}+g_4m_{03}$	$m_{44}=m_{33}+g_4m_{04}$	$m_{45}=m_{34}+g_4m_{05}$	$m_{46}=m_{35}+g_4m_{06}$	$m_{47}=m_{36}+g_4m_{07}$
c_5	$m_{50}=a_5$	$m_{51}=m_{40}+g_5m_{01}$	$m_{52}=m_{41}+g_5m_{02}$	$m_{53}=m_{42}+g_5m_{03}$	$m_{54}=m_{43}+g_5m_{04}$	$m_{55}=m_{44}+g_5m_{05}$	$m_{56}=m_{45}+g_5m_{06}$	$m_{57}=m_{46}+g_5m_{07}$
c_6	$m_{60}=a_6$	$m_{61}=m_{50}+g_6m_{01}$	$m_{62}=m_{51}+g_6m_{02}$	$m_{63}=m_{52}+g_6m_{03}$	$m_{64}=m_{53}+g_6m_{04}$	$m_{65}=m_{54}+g_6m_{05}$	$m_{66}=m_{55}+g_6m_{06}$	$m_{67}=m_{56}+g_6m_{07}$
c_7	$m_{70}=a_7$	$m_{71}=m_{60}+g_7m_{01}$	$m_{72}=m_{61}+g_7m_{02}$	$m_{73}=m_{62}+g_7m_{03}$	$m_{74}=m_{63}+g_7m_{04}$	$m_{75}=m_{64}+g_7m_{05}$	$m_{76}=m_{65}+g_7m_{06}$	$m_{77}=m_{66}+g_7m_{07}$

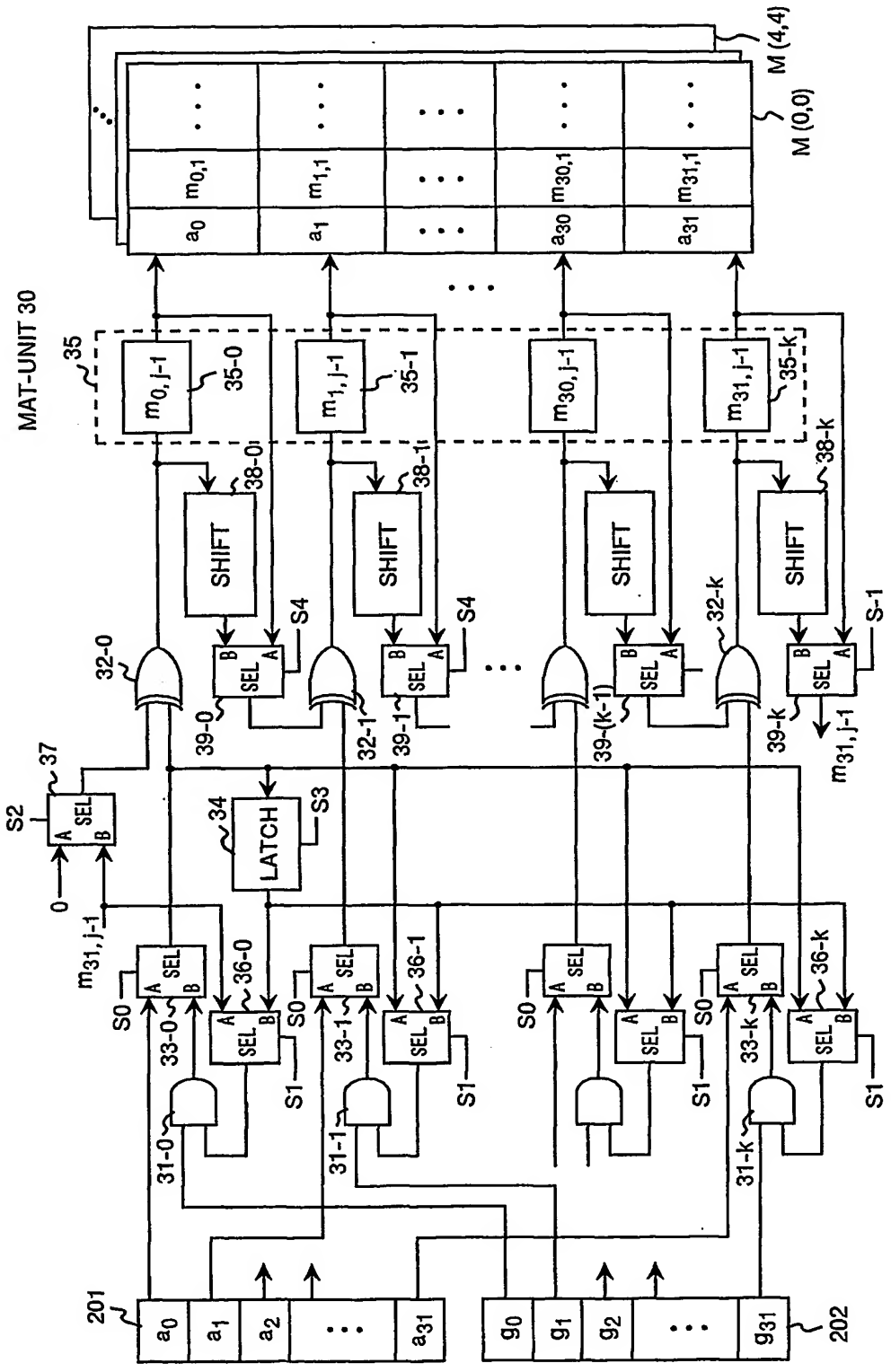
第6図


M (0, 0)
M (0, J)
M (I, 0)
M (I, J)
b_0 b_1 b_j b_{j+1}
C_0 $m_{0,0} = a_0$ $m_{0,1} = m_{n-1,0}$ $m_{0,j} = m_{n-1,j-1}$ $m_{0,j+1} = m_{n-1,j}$
C_1 $m_{1,0} = a_1$ $m_{1,1} = m_{0,0} + g_1 m_{0,1}$ $m_{1,j} = m_{0,j-1} + g_1 m_{0,j}$ $m_{1,j+1} = m_{0,j} + g_1 m_{0,j+1}$
C_{n-2} $m_{n-2,0} = a_{n-2}$ $m_{n-2,1} = m_{n-3,0} + g_{n-2} m_{0,1}$ $m_{n-2,j} = m_{n-3,j-1} + g_{n-2} m_{0,j}$ $m_{n-2,j+1} = m_{n-3,j} + g_{n-2} m_{0,j+1}$
C_{n-1} $m_{n-1,0} = a_{n-1}$ $m_{n-1,1} = m_{n-2,0} + g_{n-1} m_{0,1}$ $m_{n-1,j} = m_{n-2,j-1} + g_{n-1} m_{0,j}$ $m_{n-1,j+1} = m_{n-2,j} + g_{n-1} m_{0,j+1}$

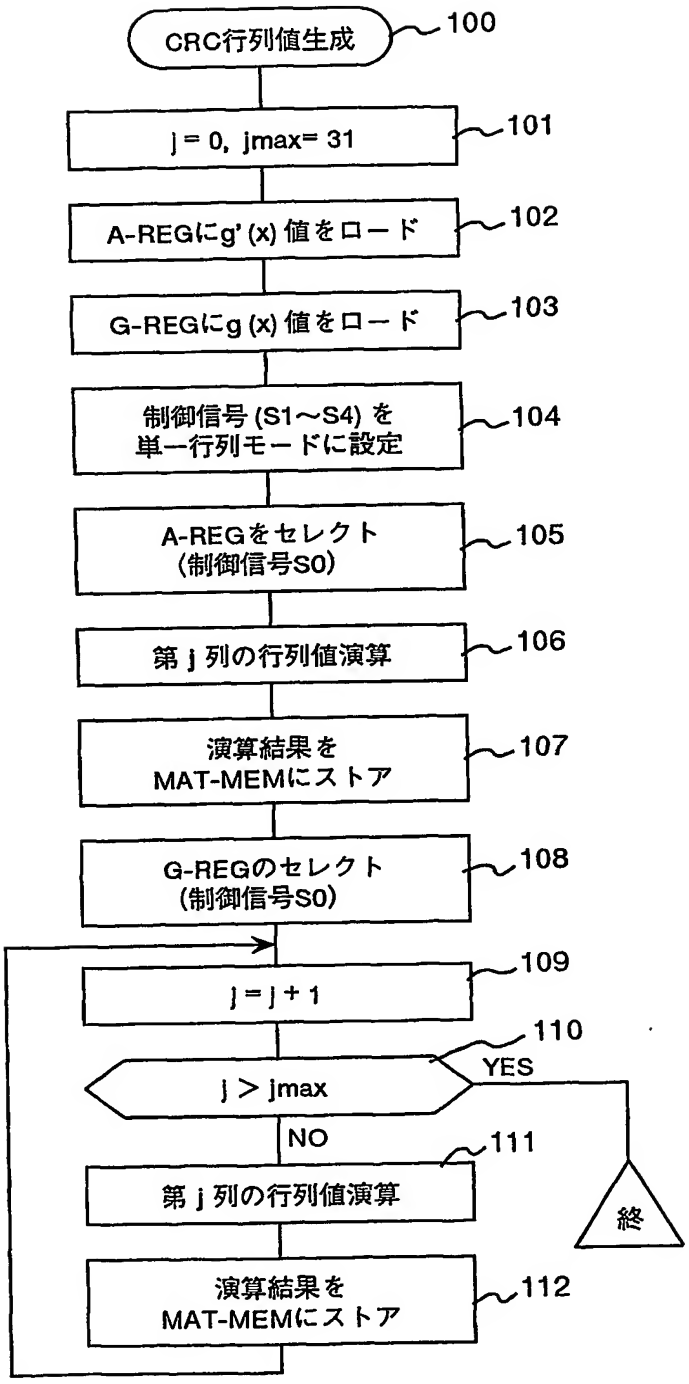
第7図


D-0
D-1
D-2
D-3
D-4
B0-B31
B31-B63
B64-B95
B96-B127
B128-B159
ECC-0
C31-C0
ECC-1
C63-C32
ECC-2
C95-C64
ECC-3
C127-C96
ECC-4
C159-C128
M(0,0)
M(0,1)
M(0,2)
M(0,3)
M(0,4)
M(1,0)
M(1,1)
M(1,2)
M(1,3)
M(1,4)
M(2,0)
M(2,1)
M(2,2)
M(2,3)
M(2,4)
M(3,0)
M(3,1)
M(3,2)
M(3,3)
M(3,4)
M(4,0)
M(4,1)
M(4,2)
M(4,3)
M(4,4)

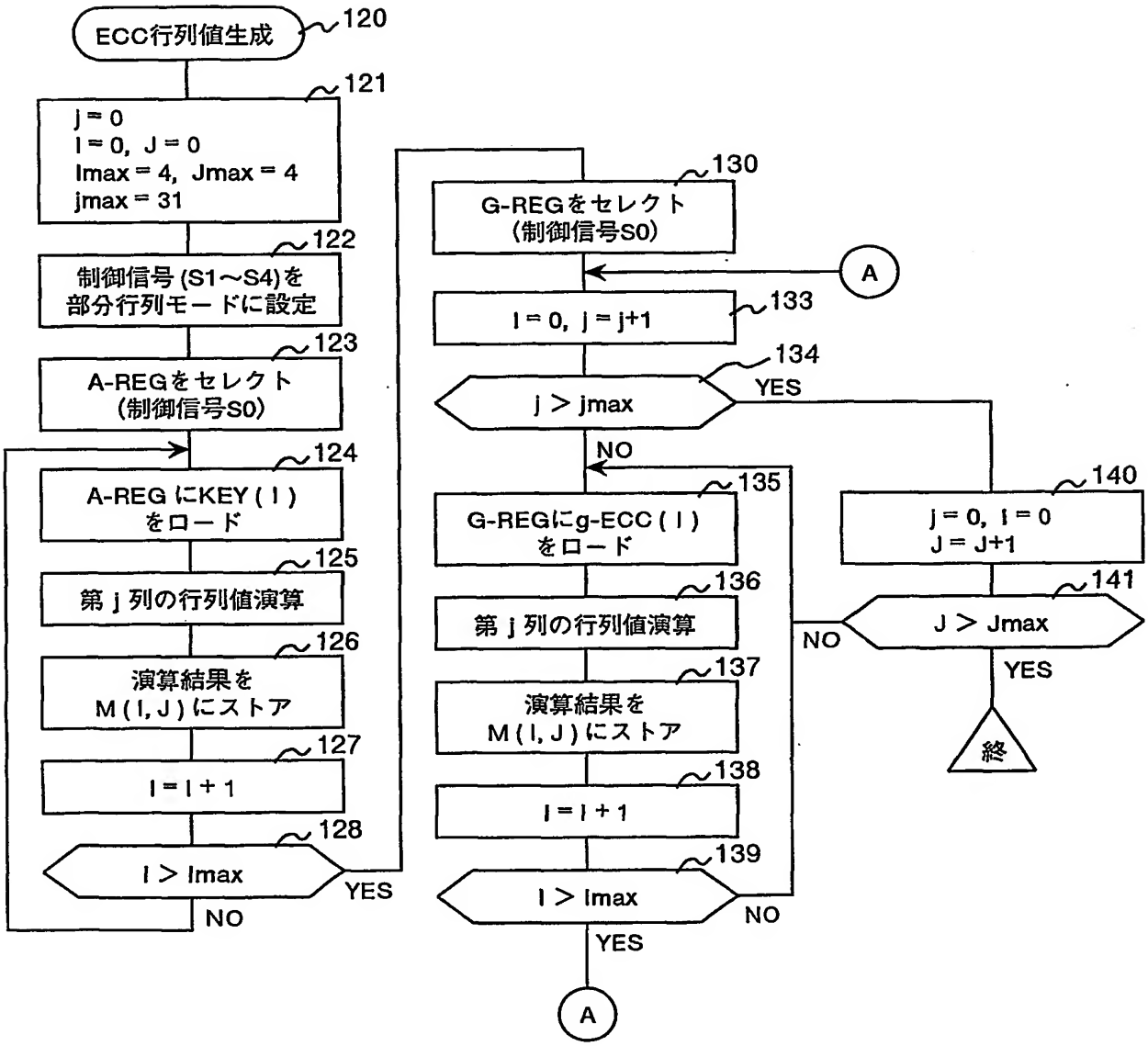
第８図



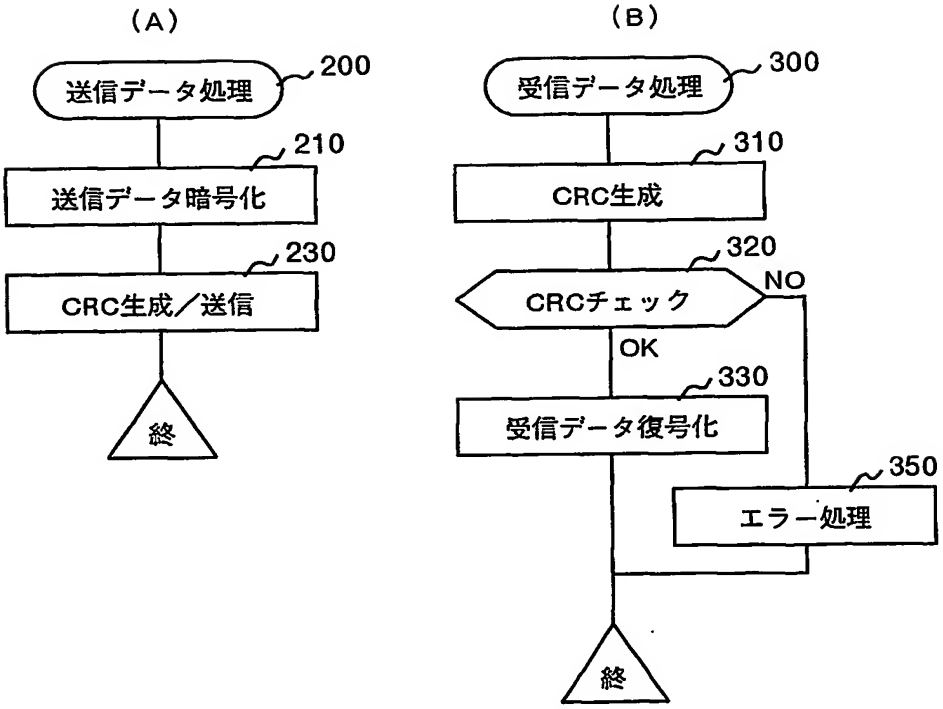
第９図


CRC行列値生成
100
j = 0, jmax= 31
101
A-REGにg' (x) 値をロード
102
G-REGにg (x) 値をロード
103
制御信号 (S1～S4) を
単一行列モードに設定
104
A-REGをセレクト
(制御信号S0)
105
第 j 列の行列値演算
106
演算結果を
MAT-MEMにストア
107
G-REGのセレクト
(制御信号S0)
108
j = j + 1
109
j > jmax
110
YES
NO
第 j 列の行列値演算
111
演算結果を
MAT-MEMにストア
112
終

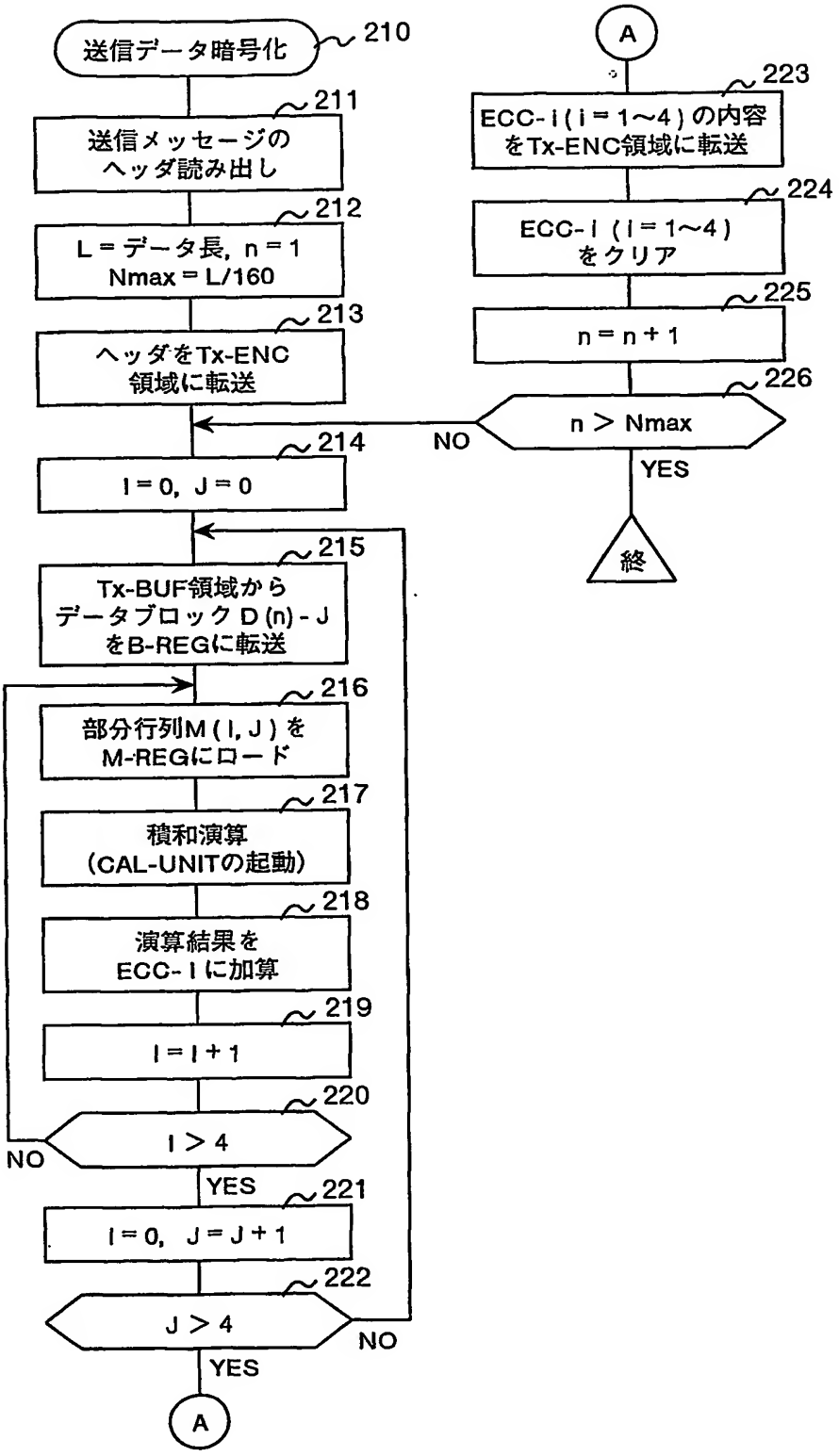
第１０図


ECC行列値生成
120
121
j = 0
I = 0, J = 0
Imax = 4, Jmax = 4
jmax = 31
122
制御信号 (S1～S4)を
部分行列モードに設定
123
A-REGをセレクト
(制御信号S0)
124
A-REG にKEY (I)
をロード
125
第 j 列の行列値演算
126
演算結果を
M (I, J) にストア
127
I = I + 1
128
I > Imax
YES
NO
130
G-REGをセレクト
(制御信号S0)
A
133
I = 0, j = j+1
134
j > jmax
YES
NO
135
G-REGにg-ECC (I)
をロード
136
第 j 列の行列値演算
137
演算結果を
M (I, J) にストア
138
I = I + 1
139
I > Imax
NO
YES
A
140
j = 0, I = 0
J = J+1
141
J > Jmax
NO
YES
終

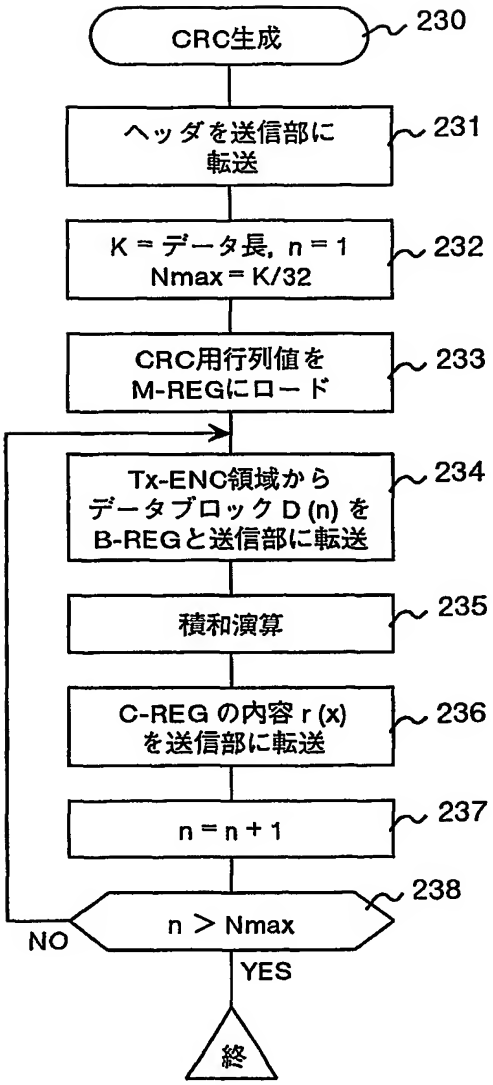
第１１図


(A)
送信データ処理
200
送信データ暗号化
210
CRC生成／送信
230
終
(B)
受信データ処理
300
CRC生成
310
CRCチェック
320
NO
OK
受信データ復号化
330
エラー処理
350
終

第１２図


送信データ暗号化
210
送信メッセージの
ヘッダ読み出し
211
L＝データ長, n＝1
Nmax＝L/160
212
ヘッダをTx-ENC
領域に転送
213
I＝0, J＝0
214
Tx-BUF領域から
データブロック D(n)-J
をB-REGに転送
215
部分行列M(I, J)を
M-REGにロード
216
積和演算
(CAL-UNITの起動)
217
演算結果を
ECC-Iに加算
218
I＝I＋1
219
I＞4
220
NO
YES
I＝0, J＝J＋1
221
J＞4
222
NO
YES
A
A
ECC-i(i＝1～4)の内容
をTx-ENC領域に転送
223
ECC-I (I＝1～4)
をクリア
224
n＝n＋1
225
n＞Nmax
226
NO
YES
終

第１３図


CRC生成
230
ヘッダを送信部に転送
231
K＝データ長, n＝1
Nmax＝K/32
232
CRC用行列値をM-REGにロード
233
Tx-ENC領域からデータブロックD(n)をB-REGと送信部に転送
234
積和演算
235
C-REGの内容r(x)を送信部に転送
236
n＝n＋1
237
n ＞ Nmax
238
NO
YES
終

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP02/06166

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G09C1/00, H03M13/15, H04L9/30, G06F11/10

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G09C1/00, H03M13/15, H04L9/30, G06F11/10

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Toroku Jitsuyo Shinan Koho 1994-2002
Kokai Jitsuyo Shinan Koho 1971-2002 Jitsuyo Shinan Toroku Koho 1996-2002

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 91/20028 A1 (MASTROVITO, Edoardo), 31 May, 1991 (31.05.91), Full text; Figs. 1 to 4 & AU 8076591 A & SE 9002124 A	1-7
Y	Kazue SHIBA, Shin'ichi KAWAMURA, Jun SHINBO, "GF(2^m) Ensan oyobi Seisu Ensan o Shori Kano na Hybrid Coprocessor no Teian", 1999nen Ango to Joho Security Symposium Yokoshu, 26 January, 1999 (26.01.99), Volume II of II, pages 819 to 824	1-7
Y	JP 2001-56640 A (Toyo Communication Equipment Co., Ltd.), 27 February, 2001 (27.02.01), Full text; Figs. 1 to 4 (Family: none)	1-7

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
20 September, 2002 (20.09.02)	08 October, 2002 (08.10.02)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP02/06166

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 7-50595 A (Toshiba Corp.), 21 February, 1995 (21.02.95), Full text; Figs. 1 to 15 & DE 69414631 C & EP 620654 A & US 5517509 A	1-7

国際調査報告

国際出願番号　PCT／JP02／06166

A.　発明の属する分野の分類（国際特許分類（IPC））

Int. Cl⁷　G09C1／00　H03M13／15　H04L9／30　G06F11／10

B.　調査を行った分野

調査を行った最小限資料（国際特許分類（IPC））

Int. Cl⁷　G09C1／00　H03M13／15　H04L9／30　G06F11／10

最小限資料以外の資料で調査を行った分野に含まれるもの

日本国実用新案公報	1922－1996年
日本国公開実用新案公報	1971－2002年
日本国登録実用新案公報	1994－2002年
日本国実用新案登録公報	1996－2002年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	WO　91／20028　A1（MASTROVITO, Edoardo） 1991.05.31　全文，FIG.1－4 ＆　AU　8076591　A　＆　SE　9002124　A	1－7
Y	斯波万恵，川村信一，新保淳；“GF（2ᵐ）演算及び整数演算を処理可能なハイブリッド・コプロセッサの提案” 1999年暗号と情報セキュリティシンポジウム予稿集， 1999.01.26，Volume II of II， p.819－824	1－7

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー

「A」特に関連のある文献ではなく、一般的技術水準を示すもの

「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの

「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）

「O」口頭による開示、使用、展示等に言及する文献

「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献

「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの

「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの

「Y」特に関連のある文献であって、当該文献と他の1以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの

「&」同一パテントファミリー文献

国際調査を完了した日　20.09.02	国際調査報告の発送日　08.10.02
国際調査機関の名称及びあて先 日本国特許庁（ISA／JP） 郵便番号100－8915 東京都千代田区霞が関三丁目4番3号	特許庁審査官（権限のある職員）　5M　4229 青木　重徳 電話番号　03－3581－1101　内線　3597

様式PCT／ISA／210（第2ページ）（1998年7月）

Ｃ（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｙ	ＪＰ　２００１－５６６４０　Ａ（東洋通信機株式会社） ２００１．０２．２７，全文，図１－４ （ファミリーなし）	１－７
Ｙ	ＪＰ　７－５０５９５　Ａ（株式会社東芝） １９９５．０２．２１　全文，図１－１５ ＆　ＤＥ　６９４１４６３１　Ｃ　＆　ＥＰ　６２０６５４　Ａ ＆　ＵＳ　５５１７５０９　Ａ	１－７